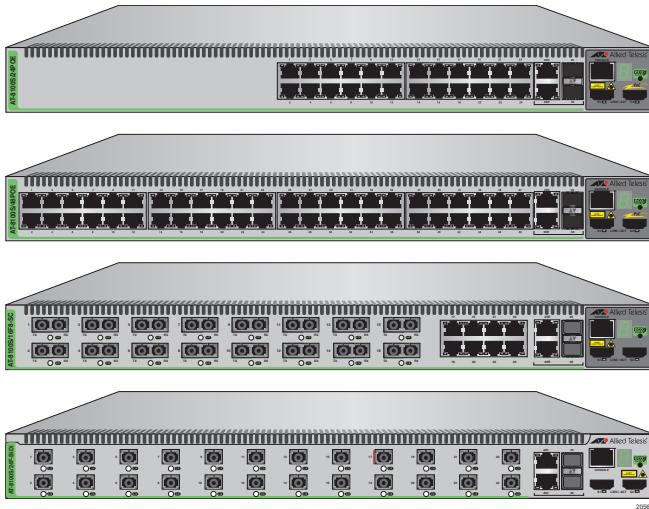


AT-8100 Series

Fast Ethernet Switches

- AT-8100L/8
- AT-8100L/8POE
- AT-8100L/8POE-E
- AT-8100S/24C
- AT-8100S/24
- AT-8100S/24POE
- AT-8100S/16F8-SC
- AT-8100S/16F8-LC
- AT-8100S/24F-LC
- AT-8100S/48
- AT-8100S/48POE



Management Software Web Browser User's Guide

AlliedWare Plus™ Version 2.2.4

613-001612 Rev. A

Copyright

Copyright © 2012, Allied Telesis, Inc.

All rights reserved.

This product includes software licensed under the BSD License. As such, the following language applies for those portions of the software licensed under the BSD License:

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Allied Telesis, Inc. nor the names of the respective companies above may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Copyright 1989, 1991, 1992 by Carnegie Mellon University. Derivative Work - 1996, 1998-2000. Copyright 1996, 1998-2000 by The Regents of the University of California - All rights reserved. Copyright (c) 2001-2003 by Networks Associates Technology, Inc. - All rights reserved. Copyright (c) 2001-2003 by Cambridge Broadband Ltd. - All rights reserved. Copyright (c) 2003 by Sun Microsystems, Inc. - All rights reserved. Copyright (c) 2003-2005 by Sparta, Inc. - All rights reserved. Copyright (c) 2004 by Cisco, Inc. and Information Network Center of Beijing University of Posts and Telecommunications. - All rights reserved. Copyright (c) 2003 by Fabasoft R&D Software GmbH & Co KG - All rights reserved. Copyright (c) 2004-2006 by Internet Systems Consortium, Inc. ("ISC") - All rights reserved. Copyright (c) 1995-2003 by Internet Software Consortium - All rights reserved. Copyright (c) 1992-2003 by David Mills - All rights reserved. Copyright (c) 1995 by Tatu Ylonen <ylo@cs.hut.fi>, Espoo, Finland - All rights reserved. Copyright (c) 1998 by CORE SDI S.A., Buenos Aires, Argentina - All rights reserved. Copyright 1995, 1996 by David Mazieres - All rights reserved. Copyright 1983, 1990, 1992, 1993, 1995 by The Regents of the University of California - All rights reserved. Copyright (c) 1995 Patrick Powell - All rights reserved. Copyright (c) 1998-2005 The OpenSSL Project - All rights reserved. Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com) - All rights reserved. Copyright (c) 2008, Henry Kwok - All rights reserved. Copyright (c) 1995, 1998, 1999, 2000, 2001 by Jef Poskanzer <jef@mail.acme.com>. - All rights reserved.

Some components of the SSH software are provided under a standard 2-term BSD license with the following names as copyright holders: Markus Friedl, Theo de Raadt, Niels Provos, Dug Song, Aaron Campbell, Damien Miller, Kevin Steves, Daniel Kouril, Wesley Griffin, Per Allansson, Nils Nordman, and Simon Wilkinson,

Portable OpenSSH includes code from the following copyright holders, also under the 2-term BSD license: Ben Lindstrom, Tim Rice, Andre Lucas, Chris Adams, Corinna Vinschen, Cray Inc., Denis Parker, Gert Doering, Jakob Schlyter, Jason Downs, Juha Yrjola, Michael Stone, Network Associates, Solar Designer, Todd C. Miller, Wayne Schroeder, William Jones, Darren Tucker, Sun Microsystems, The SCO Group.

Some Portable OpenSSH code is licensed under a 3-term BSD style license to the following copyright holders: Todd C. Miller, Theo de Raadt, Damien Miller, Eric P. Allman, The Regents of the University of California, and Constantin S. Svintsoff. Some Portable OpenSSH code is licensed under an ISC-style license to the following copyright holders: Internet Software Consortium, Todd C. Miller, Reyk Floeter, and Chad Mynhier. Some Portable OpenSSH code is licensed under a MIT-style license to the following copyright holder: Free Software Foundation, Inc.

This product also includes software licensed under the GNU General Public License available from:

<http://www.gnu.org/licenses/gpl2.html>

Allied Telesis is committed to meeting the requirements of the open source licenses including the GNU General Public License (GPL) and will make all required source code available.

If you would like a copy of the GPL source code contained in this product, please send us a request by registered mail including a check for US\$15 to cover production and shipping costs, and a CD with the GPL code will be mailed to you.

GPL Code Request

Allied Telesis, Inc.

3041 Orchard Parkway

San Jose, California 95134

No part of this publication may be reproduced without prior written permission from Allied Telesis, Inc.

Allied Telesis, AlliedWare Plus, and the Allied Telesis logo are trademarks of Allied Telesis, Incorporated. Microsoft and Internet Explorer are registered trademarks of Microsoft Corporation. All other product names, company names, logos or other designations mentioned herein are trademarks or registered trademarks of their respective owners.

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Preface	15
Document Conventions	16
Downloading Management Software and Web-based Guides	17
Contacting Allied Telesis	18
Online Support	18
Email and Telephone Support	18
Returning Products	18
Sales or Corporate Information	18
Management Software Updates	18
Chapter 1: AlliedWare Plus™ Version 2.2.4 Web Browser Interface	19
Management Sessions	20
Web Manager Accounts	21
Chapter 2: Starting a Management Session	23
Non-secure HTTP and Secure HTTPS Modes	24
HTTP Mode	24
HTTPS Mode	24
Starting the Initial Web Management Session	25
Logging on to the Switch	27
What to Configure First	30
Changing the Login Password	30
Assigning a Name to the Switch	30
Changing a Management IP Address	30
Setting System Time	31
Starting a Web Management Session	32
When You Do Not Know the IP Address of the Switch	32
When the Switch Does Not Display the Login Page	33
Logging on to the CLI through the Console Port	33
Checking for the IP Addresses of the Switch in the CLI	34
Adding an IP Address to the Switch in the CLI	34
Checking the Status of HTTP and HTTPS Services in the CLI	34
Enabling HTTP or HTTPS Service in the CLI	35
Saving your Changes in the CLI	36
Saving Your Changes	37
Ending a Web Management Session	38
Chapter 3: Basic Switch Parameters	39
Setting the System Date and Time	40
Configuring an SNTP or NTP Server	40
Setting System Time Manually	42
Configuring a Telnet or SSH Server	45
Configuring a Remote Log Server	47
Setting the Switch Information	48
Managing the Configuration File	50
Displaying the Configuration Files	50
Setting the Active Configuration File	51

Downloading a Configuration File onto Your PC	51
Deleting a Configuration	52
Managing Local User Accounts	53
Adding a New User Account.....	53
Changing a User Password.....	55
Changing the User Privilege.....	56
Deleting a User Account.....	57
Rebooting a Switch	59
Upgrading the Software	60
Returning the AlliedWare Plus Management Software to the Factory Default Values.....	63
Displaying System Information	64
Chapter 4: Setting Port Parameters	67
Port Numbers on the Switch	68
Displaying the Port Parameters	69
Changing the Port Settings	72
Displaying the Storm Control Settings	76
Modifying the Storm Control Settings	78
Chapter 5: Setting Port Statistics	81
Displaying Port Statistics	82
Displaying Transmit and Receive Port Statistics	82
Displaying Receive Statistics.....	83
Displaying Transmit Statistics.....	85
Displaying Interface Statistics.....	87
Clearing Port Statistics.....	89
Reloading Statistics	90
Chapter 6: Port Mirroring	91
Overview	92
Displaying Port Mirroring Settings.....	93
Assigning a Destination Port.....	95
Assigning Source Ports and Port Mirroring Values	96
Deleting Port Mirroring Settings	98
Chapter 7: Spanning Tree Protocol on a Port	99
Overview	100
Displaying Port Spanning Tree Protocol Settings	101
Modifying Port Spanning Tree Protocol Settings	103
Chapter 8: Setting the MAC Address	107
Displaying the Unicast MAC Addresses	108
Displaying the Multicast MAC Addresses	110
Assigning a Unicast MAC Address	111
Assigning a Multicast MAC Address	113
Deleting a Unicast MAC Address.....	115
Deleting a Multicast MAC Address	116
Chapter 9: Link Aggregation Control Protocol (LACP)	117
Overview	118
Displaying LACP Trunks	119
Adding an LACP Trunk	121
Modifying an LACP Trunk	123
Deleting an LACP Trunk	125
Chapter 10: Setting Static Port Trunks	127
Overview	128
Displaying Static Trunk Settings	129

Adding Static Trunks	131
Modifying the Static Trunk Settings	134
Deleting Static Trunks	137
Chapter 11: Setting Port-based and Tagged VLANs	139
Overview.....	140
Port-based VLANs	140
Port VLAN Identifier	140
Tagged VLANs.....	140
Tagged and Untagged Ports.....	141
Native VLAN.....	141
Displaying VLANs	142
Adding an VLAN	143
Modifying VLANs	145
Assigning a Native VLAN	148
Removing an Untagged Port from a VLAN.....	150
Deleting VLANs	152
Chapter 12: Spanning Tree Protocols on the Switch	153
Overview.....	154
Displaying and Modifying Spanning Tree Protocol Settings on the Switch	155
Chapter 13: Internet Group Management Protocol (IGMP) Snooping	159
Overview.....	160
Displaying and Modifying IGMP Snooping Configuration.....	161
Disabling IGMP Snooping	164
Displaying the Routers List.....	165
Clearing the Routers List	167
Displaying the Hosts List	168
Chapter 14: IGMP Snooping Querier	171
Overview.....	172
Assigning Multiple Queriers	173
Guidelines.....	176
Displaying IGMP Snooping Querier.....	177
Modifying IGMP Snooping Query Interval	179
Chapter 15: Power Over Ethernet (PoE)	181
Overview.....	182
Power Sourcing Equipment (PSE).....	182
Powered Device (PD).....	182
PD Classes	182
Port Prioritization.....	183
Displaying PoE Port Settings.....	184
Modifying PoE Settings Globally	187
Modifying PoE Settings on a Port.....	188
Chapter 16: MAC Address-based Port Security	191
Overview.....	192
Static Versus Dynamic Addresses	192
Intrusion Actions.....	192
Guidelines	193
Displaying the MAC Address-based Port Security Settings	194
Modifying the MAC Address-based Port Security Settings	196
Disabling MAC Address-based Port Security Settings	198
Chapter 17: RADIUS and TACACS+ Clients	199
Overview.....	200

Remote Manager Accounts	200
Accounting Information.....	201
Configuring RADIUS and TACACS+	201
Placing RADIUS and TACACS+ Servers in the Client's List.....	201
Configuring RADIUS for Remote Manager Authentication	203
Configuring Remote Manager Authentication Using RADIUS.....	203
Adding a RADIUS Server	206
Configuring TACACS+ for Remote Manager Authentication	208
Configuring Remote Manager Authentication Using TACACS+.....	208
Adding a TACACS+ Server	211
Deleting an Authentication Server	213
Chapter 18: 802.1x Port-based Network Access	215
Overview	216
Port Roles.....	216
Operating Modes.....	217
Dynamic VLAN Assignments.....	219
Guest VLAN.....	220
Enabling 802.1x Port-based Authentication on the Switch	221
Configuring 802.1x Port-based Authentication	222
Disabling 802.1x Port-based Authentication on the Switch	227
Disabling 802.1x Port-based Authentication on a Port	228
Chapter 19: Setting IPv4 and IPv6 Addresses	229
Overview	230
IP Management Guidelines	231
Displaying IPv4 Interfaces	232
Adding an IPv4 Address	234
Changing an IPv4 Address	236
Deleting an IPv4 Address	238
Displaying the IPv6 Interface	239
Adding an IPv6 Address	241
Changing IPv6 Addresses	243
Deleting IPv6 Addresses.....	245
Chapter 20: Access Control Lists (ACL)	247
Overview	248
Classifier Number Ranges.....	248
Filtering Criteria	248
IPv4 Address and Mask.....	249
Actions	249
How Ingress Packets are Compared Against ACLs	249
Guidelines.....	250
Creating an ACL	251
Assigning an ACL to Ports	255
Displaying a List of ACLs	257
Chapter 21: Setting Static Routes	259
Displaying Static Routes	260
Adding a Static Route	262
Deleting a Static Route	264
Displaying the Routing Table	265
Chapter 22: Quality of Service (QoS)	267
Overview	268
Class Information.....	268
Priority Queue.....	268

Classifier Number Ranges	268
Filtering Criteria.....	269
Actions	269
How Ingress Packets are Selected with Filtering Criteria	269
Guidelines	269
Creating a QoS Policy	271
Assigning a QoS Policy to Ports.....	276
Displaying a List of QoS Policies.....	278
Chapter 23: Setting Dynamic Routes Using RIP	279
Overview.....	280
Enabling RIP	280
Displaying the RIP Configuration.....	281
Enabling RIP on a VLAN Interface	283
Changing the RIP Settings	286
Removing a VLAN Interface from the RIP Configuration	287
Displaying RIP Statistics.....	288
Reloading RIP Statistics	290
Chapter 24: Managing the ARP Table	291
Overview.....	292
ARP Table Management Guidelines.....	292
Displaying the ARP Table.....	293
Adding a Static ARP Entry.....	295
Deleting ARP Entries	297
Chapter 25: LLDP and LLDP-MED	299
Overview.....	300
Enabling and Configuring LLDP on the Switch.....	302
Disabling LLDP on the Switch	305
Configuring LLDP on a Port.....	306
Selecting LLDP TLVs on a Port.....	308
Setting a Location Entry for the LLDP-MED Location TLV	312
Creating a Civic Location Entry.....	312
Creating a Coordinate Location	316
Creating an Emergency Location Identification Number (ELIN) Location.....	319
Assigning LLDP Locations to a Port.....	322
Selecting LLDP-MED TLVs on a Port.....	324
Displaying LLDP Neighbor Information	327
Displaying LLDP Statistics.....	329
Displaying Location Entries	332
Displaying Civic Locations	332
Displaying Coordinate Locations.....	333
Displaying ELIN Locations	334
Displaying LLDP and LLDP-MED Settings	335
Displaying the Basic LLDP Configuration	335
Displaying LLDP Port Assignments	336
Displaying Port Locations.....	337
Displaying LLDP TLV	337
Displaying LLDP-MED TLV	339
Chapter 26: sFlow	341
Overview.....	342
Ingress Packet Samples	342
Packet Counters.....	342
sFlow Collectors.....	343
Guidelines	343

Contents

Configuring sFlow on a Port.....	344
Specifying an sFlow Collector.....	346
Enabling sFlow on the Switch	348
Displaying the sFlow Settings	349

Figures

Figure 1: Login Page	26
Figure 2: Login Page with Entries.....	27
Figure 3: Dashboard Page	28
Figure 4: AlliedWare Plus™ Command Line Prompt.....	34
Figure 5: Displaying the IP Address	34
Figure 6: Displaying the Status of HTTP Service	35
Figure 7: Displaying the Status of HTTPS Service	35
Figure 8: System Contact Information Page.....	37
Figure 9: System Settings Tab	41
Figure 10: System Time Settings Page with Network Time Settings Tab	41
Figure 11: System Time Settings Page with Date & Time Tab.....	43
Figure 12: Calendar Page	44
Figure 13: System Services Page	45
Figure 14: System Contact Information Page.....	48
Figure 15: Configuration Files Page	50
Figure 16: File Download Popup Window of Internet Explorer 8.....	51
Figure 17: User Management Page.....	54
Figure 18: User Management Page with Change Password Tab.....	55
Figure 19: User Management Page with Change Privilege Tab.....	56
Figure 20: User Management Page with Delete User Tab	58
Figure 21: User Login page on the Allied Telesis Website	60
Figure 22: System Upgrade Page	61
Figure 23: Port Number	68
Figure 24: Switching Tab with Port Tab.....	69
Figure 25: Port Configuration Page	70
Figure 26: Port Configuration Modify Page.....	73
Figure 27: Storm Control List Page	76
Figure 28: Storm Control Settings Page	78
Figure 29: Port Statistics Page with Tx + Rx Tab	82
Figure 30: Port Statistics with the Receive Tab	84
Figure 31: Port Statistics with the Transmit Tab.....	86
Figure 32: Port Statistics Page with Interface Tab.....	87
Figure 33: Port Statistics Page with the Reload Page Button.....	90
Figure 34: Port Mirroring List Page	93
Figure 35: Modify Port Mirroring Page.....	96
Figure 36: Port Spanning Tree Settings Page	101
Figure 37: Modify Port Spanning Tree Settings Page	103
Figure 38: Switching Tab	108
Figure 39: Unicast MACs Page	108
Figure 40: Multicast MACs Page	110
Figure 41: Unicast MAC Address Page	111
Figure 42: Multicast MAC Address Page	113
Figure 43: Switching Tab with Link Aggregation Selected.....	119
Figure 44: LACP Trunks Page.....	119
Figure 45: Add LACP Trunk Page	121
Figure 46: Modify LACP Trunk Page	123
Figure 47: Switching Tab with Static Trunks.....	129
Figure 48: Static Trunks Page	129
Figure 49: Add Static Trunk Page	132
Figure 50: Modify Static Trunk Page	135

Figures

Figure 51: VLANs Page	142
Figure 52: Add VLAN Page	143
Figure 53: Modify VLAN Page	146
Figure 54: Native VLAN Page	148
Figure 55: Modify VLAN Page	151
Figure 56: Spanning Tree Settings Page	155
Figure 57: Switching IGMP Tab	161
Figure 58: IGMP Snooping Page with Configuration Tab	162
Figure 59: IGMP Snooping Page with Routers List Tab	165
Figure 60: IGMP Snooping Page with Hosts List Tab	168
Figure 61: IGMP Snooping Querier with One Querier	173
Figure 62: IGMP Snooping Querier with Two Queriers	174
Figure 63: Switching IGMP Tab	177
Figure 64: IGMP Snooping Querier Page	177
Figure 65: Edit IGMP Snooping Querier Page	179
Figure 66: Switching Tab	184
Figure 67: PoE Port List Page	185
Figure 68: Modify Port PoE Settings Page	188
Figure 69: Security Tab	194
Figure 70: MAC Based Port Security Page	194
Figure 71: Modify MAC Based Port Security Page	196
Figure 72: Authentication Server Configuration Page with RADIUS Tab	204
Figure 73: Radius Add Page	206
Figure 74: Authentication Server Configuration Page with TACACS+ Tab	209
Figure 75: TACACS+ Add Page	212
Figure 76: Example of Port Roles	217
Figure 77: Single Host Mode	217
Figure 78: Multiple Host Operating Mode	218
Figure 79: Multiple Supplicant Mode	219
Figure 80: 802.1x Authentication Page	221
Figure 81: Modify 802.1x Authentication Page	222
Figure 82: Modify 802.1x Authentication Page Expanded	223
Figure 83: 802.1x Authentication Page with Status Enabled	227
Figure 84: Layer 3 Tab	232
Figure 85: IPv4 Interfaces Page	232
Figure 86: IP Address Configuration Page	234
Figure 87: Edit IP Address Configuration Page	236
Figure 88: Layer 3 Tab	239
Figure 89: IPv6 Interface Page	239
Figure 90: IPv6 Management Configuration Page	241
Figure 91: Edit IPv6 Management Configuration Page	243
Figure 92: ACLs and QoS Tab	251
Figure 93: Traffic Classifiers Page	251
Figure 94: Traffic Classification Page	252
Figure 95: Text box for Mirror to Port	253
Figure 96: Policies/ACLs Page	255
Figure 97: Traffic Classifiers Page	256
Figure 98: Traffic Classifiers Page	257
Figure 99: Layer 3 Tab	260
Figure 100: Static Routes Page	260
Figure 101: Add Static ARP Page	262
Figure 102: Layer 3 Tab	265
Figure 103: Routing Table Page	265
Figure 104: ACLs and QoS Tab	271
Figure 105: Traffic Classifiers Page	271
Figure 106: Traffic Classification Page	272
Figure 107: Text box for Priority Queue	273
Figure 108: Text box for DSCP	273
Figure 109: Text box for CoS	274
Figure 110: Policies/ACLs Page	276

Figure 111: Traffic Classifier Page	277
Figure 112: Traffic Classifiers Page.....	278
Figure 113: Layer 3 Tab	281
Figure 114: RIP Configuration Page.....	281
Figure 115: Layer 3 Tab	283
Figure 116: RIP Interface Page	284
Figure 117: Layer 3 Tab	288
Figure 118: RIP Configuration Page.....	288
Figure 119: RIP Statistics Page with the Refresh Button	290
Figure 120: Switching Tab	293
Figure 121: ARP Table Page.....	293
Figure 122: Add Static ARP Page	295
Figure 123: Discovery & Monitoring Tab	302
Figure 124: LLDP Configuration Page.....	303
Figure 125: LLDP Port Config Page	306
Figure 126: Modify LLDP Port Configuration Page.....	307
Figure 127: LLDP TLV Tab.....	308
Figure 128: LLDP TLV Page	309
Figure 129: Modify LLDP TLV Page	310
Figure 130: Locations Tab	313
Figure 131: LLDP Civic Location Page.....	313
Figure 132: LLDP Civic Location Page— Modify.....	314
Figure 133: LLDP Coordinate Location Page.....	317
Figure 134: LLDP Coordinate Location Page— Modify.....	318
Figure 135: LLDP ELIN Location List Page	320
Figure 136: LLDP ELIN Location Page	320
Figure 137: LLDP Port Location Page	322
Figure 138: Modify LLDP Port Location Page	323
Figure 139: LLDP-MED TLV Page	324
Figure 140: Modify LLDP-MED TLV Page	325
Figure 141: LLDP Neighbors Information Page	327
Figure 142: LLDP Statistics Page with Port Statistics Tab	329
Figure 143: LLDP Statistics Page with Summary Tab	330
Figure 144: Discovery &Monitoring Tab	344
Figure 145: sFlow Page with the Port Configurations Tab	344
Figure 146: sFlow Port Modify Page.....	345
Figure 147: sFlow Page with Collectors Tab	346
Figure 148: sFlow Collector Page...	347

Figures

Preface

This manual is the web browser management guide for the AT-8100 Series of Fast Ethernet switches. The instructions in this guide explain how to start a management session, use the web interface of the AlliedWare Plus™ Management Software, and configure the features of the switch.

For hardware installation instructions, refer to the *AT-8100L and 8100S Series Fast Ethernet Stand-alone Installation Guide* and *AT-8100 Series Fast Ethernet Switches Stack Installation Guide*.

This preface contains the following sections:

- “Document Conventions” on page 16
- “Downloading Management Software and Web-based Guides” on page 17
- “Contacting Allied Telesis” on page 18



Caution

The software described in this document may contain certain encryption/security or cryptographic functionality and for exporting those products/software, USA export restrictions apply as per 15 C.F.R. Part 730-772 (particularly Part 740.17). At present, as per United States of America's export regulations our products/software cannot be exported to Cuba, Iran, North Korea, North Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please refer to export regulations of USA.

Document Conventions

This document uses the following conventions:

Note

Notes provide additional information.



Caution

Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.



Warning

Warnings inform you that performing or omitting a specific action may result in bodily injury.

Downloading Management Software and Web-based Guides

Both new releases of management software and product documentation are available from the Allied Telesis web sites. The management software is available at www.alliedtelesis.com/support/software. To display all of the network management software for a product, use the pull-down menu labeled "All" to select a hardware product model such as "AT-8100S/24." Then double click the software version that you want to download onto your local work station or server.

The installation and user guides for all Allied Telesis products are available in PDF at www.alliedtelesis.com/support/documentation/. To display all of the product documentation for a product, use the pull-down menu labeled "All" to select a hardware product model such as "AT-8100S/48." Then double click the document that you want to view. You can view the documents online or download them onto your local workstation or server.

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support and for sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: www.alliedtelesis.com/support/kb.aspx. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Allied Telesis web site at www.alliedtelesis.com. Select your country from the list on the web site and then select the appropriate tab.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender's expense. For instructions on how to obtain an RMA number, go to our web site at www.alliedtelesis.com and then select Support and Replacement Services.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at www.alliedtelesis.com.

Management Software Updates

New releases of the management software for our managed products are available from the Allied Telesis web site: www.alliedtelesis.com. For downloading instructions, see "Downloading Management Software and Web-based Guides" on page 17.

Chapter 1

AlliedWare Plus™ Version 2.2.4 Web Browser Interface

This chapter describes the types of management sessions using the AlliedWare Plus™ management software and the Web interface manager accounts. See the following sections:

- “Management Sessions” on page 20
- “Web Manager Accounts” on page 21

Management Sessions

The AT-8100 series switches provide two management interfaces: the AlliedWare Plus™ Web interface and Command Line Interface (CLI). This manual provides procedures that guide you through the AlliedWare Plus™ Web interface.

The initial management session of the switch can be from a management session either through the Web interface or the CLI. The switch is shipped from the factory with an IP address assigned and the Web interface (HTTP service) enabled so that you can start the initial management session through the Web interface. To start the initial web management session, see Chapter 2, “Starting a Management Session” on page 23.

The web interface allows access to a subset of the AlliedWare Plus features. For access to all of the AlliedWare Plus features, you must use the CLI.

Detailed feature descriptions are not provided in this guide. For thorough explanations of the features, see the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*.

Web Manager Accounts

You must log on to manage the switch. This requires a valid username and password. The switch comes with one manager account with a username of “manager” and the default password of “friend.” Both the username and password are case sensitive. This account gives you access to all management modes and commands.

In the Web interface, you can create two additional remote manager accounts. For instructions, see “Managing Local User Accounts” on page 53. The switch supports up to three manager sessions at one time.

Chapter 2

Starting a Management Session

This chapter describes how to start a management session using the AlliedWare Plus™ Web interface as well as how to select fields, save your changes, and end a management session. See the following sections:

- “Non-secure HTTP and Secure HTTPS Modes” on page 24
- “Starting the Initial Web Management Session” on page 25
- “Logging on to the Switch” on page 27
- “What to Configure First” on page 30
- “Starting a Web Management Session” on page 32
- “Saving Your Changes” on page 37
- “Ending a Web Management Session” on page 38

For additional information about the web server, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Non-secure HTTP Web Browser Server
- Non-secure HTTP Web Browser Server Commands
- Secure HTTPS Web Browser Server
- Secure HTTPS Web Browser Server Commands
- Starting a Management Session

Non-secure HTTP and Secure HTTPS Modes

The switch has a web browser server so that you can remotely manage the switch over the network from a web browser on your PC. The server can operate in either plain-text HTTP mode or encrypted HTTPS mode. To access the switch through a web browser on your PC, either HTTP service or HTTPS service must be enabled.

HTTP Mode

Web browser management sessions of the switch conducted in the HTTP mode are non-secure because the packets exchanged by the server on the switch and your management workstation are sent in clear text, leaving the packets vulnerable to snooping.

The switch shipped from the factory is configured with HTTP service enabled.

HTTPS Mode

Web browser management sessions of the switch conducted in the HTTPS mode are protected against snooping because the packets exchanged between the switch and your management workstation are encrypted. Only the switch and the workstation are able to decipher the packets.

To access the switch in the HTTPS mode:

- The switch must have a HTTPS certificate.
- HTTPS service on the switch must be enabled.

Note

Either HTTPS or HTTP service can be enabled at the same time. To enable HTTPS service, HTTP must be disabled.

To configure the switch with a HTTPS certificate and enable HTTPS service, you must use the AlliedWare Plus™ Command Line Interface (CLI). See “Secure HTTPS Web Browser Server” chapter in *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*.

Starting the Initial Web Management Session

This section explains how to start a management session for the first time using the AlliedWare Plus™ Web interface. The switch shipped from the factory is configured with an IP address assigned and the Web interface (HTTP service) enabled.

The switch and your PC must be directly connected through an twisted-pair cable, and the IP addresses of the switch and your PC must be members of the same network. Because the switch is shipped from the factory with the IP address 169.254.1.1 and the subnet mask 16, you must assign your PC an IP address in the 169.254.0.0/16 network except 169.254.1.1. In addition, your PC must have a web browser, such as Windows Explorer, installed.

There are two ways to assign an IP address to your PC:

- Manually assign any IP address in the 169.254.0.0/16 network (except 169.254.1.1) to your PC.
- Disconnect your PC from a network and let your PC automatically set an IP address in the 169.254.0.0/16 network. When a PC is disconnected from a network and no longer connected to a DHCP server, Windows assigns a random IP address in the 169.254.0.0/16 network to the PC.

Note

If you delete the boot.cfg file and reboot the switch, the factory default settings are lost. Deleting the boot.cfg file and restarting the switch restores the switch to its default configuration with HTTP service disabled and no IP address assigned.

To start a Web management session when the switch has the default configuration settings, you must use the AlliedWare Plus™ Command Line Interface (CLI) to assign an IP address and enable HTTP or HTTPS service. For more information about enabling HTTP or HTTPS service and assigning an management IP address, see “Starting a Web Management Session” on page 32.”

To start a Web management session using a PC with an IP address in the 169.254.0.0/16 network, perform the following procedure:

1. Connect a RJ-45 plug on a straight-through twisted-pair cable to a twisted-pair port on the switch.
2. Connect the other RJ-45 plug on the straight-through twisted-pair cable to a twisted-pair connector on the PC.

3. Open a web browser on the PC and enter the following:

<http://169.254.1.1>

The AT-8100 Login page is displayed as shown in Figure 1.



Figure 1. Login Page

Logging on to the Switch

Once you start the Web interface, the AT-8100 Login page is displayed.

Enter “manager” in the User Name field and “friend” in the Password field as shown in Figure 2. Then click the **Login** button.



Figure 2. Login Page with Entries

The Dashboard page is displayed. See Figure 3. The Dashboard page is the home page of the switch.

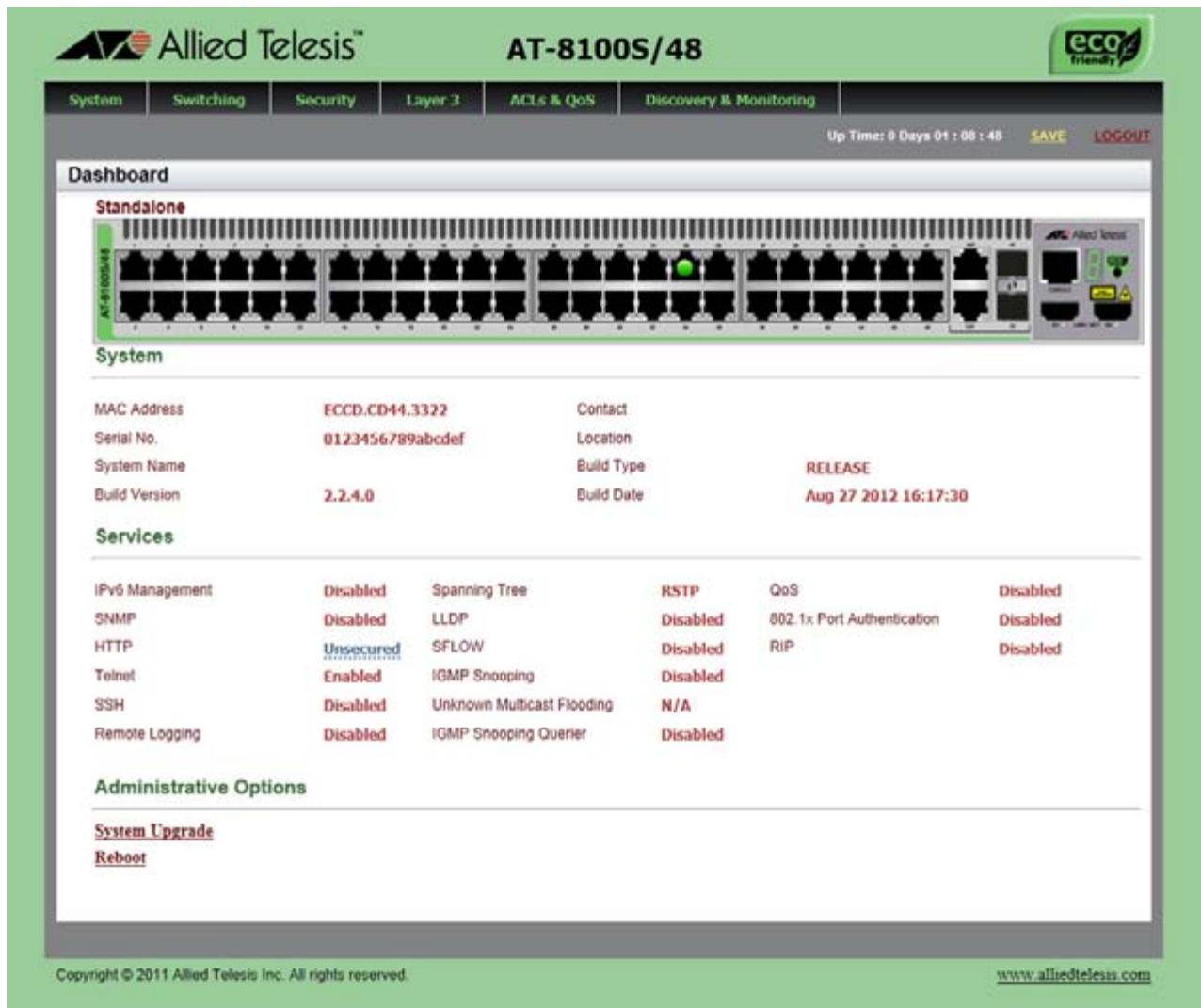


Figure 3. Dashboard Page

The following fields are displayed:

- Up Time**— Indicates the length of time since the switch was last reset or power cycled in days, hours, minutes and seconds.

Note

Up Time is displayed on the top-right corner of the screen.

The System section displays the following information:

- MAC Address**— Indicates the MAC address of the switch.
- Serial No.**— Lists the unique serial number of the switch.
- System Name**— Indicates the name of the switch. To specify this field, see Setting the Switch Information.

- Version**— Indicates the software version number of the AlliedWare Plus Management Software.
- Contact**— Indicates the contact person for the switch. To specify this field, see Setting the Switch Information.
- Location**— Indicates the location of the switch. To specify this field, see Setting the Switch Information.

The Services section displays the following information:

- IPv6 Management**— Indicates if the IPv6 Management is enabled or disabled on the switch.
- SNMP**— Indicates the SNMP setting of the switch.
- HTTP**— Indicates the HTTP setting of the switch.
- Telnet**— Indicates if Telnet is enabled or disabled on the switch.
- SSH**— Indicates if SSH is enabled or disabled on the switch.
- Remote Logging**— Indicates if the remote logging is enabled or disabled on the switch.
- Spanning Tree**— Indicates if STP, RSTP, or MSTP is enabled on the switch. The default setting is “RSTP.”
- QoS**— Indicates if QoS is enabled or disabled on the switch.
- LLDP**— Indicates if LLDP is enabled or disabled on the switch.
- sFLOW**— Indicates if sFlow is enabled or disabled on the switch.
- IGMP Snooping**— Indicates if IGMP Snooping is enabled or disabled on the switch.
- IGMP Snooping Querier**— Indicates if IGMP Snooping Querier is enabled or disabled on the switch.
- 802.1x Port Authentication**— Indicates if 802.1x Port Authentication is enabled or disabled on the switch.
- RIP**— Indicates if RIP is enabled or disabled on the switch.

The Administration Options section displays the following information:

- System Upgrade**— Select this field to upgrade your system software. See “Upgrading the Software” on page 60.
- Reboot**— Select this field to reboot the switch. For instructions, see “Rebooting a Switch” on page 59.

What to Configure First

Here are a few suggestions on what to configure during your initial management session on the switch through the Web interface. The initial management session can be performed through the Command Line Interface (CLI) as well as the Web interface. For instructions on how to start a local management session through the CLI, refer to *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User's Guide*.

Changing the Login Password

To protect the switch from unauthorized access, change the password of the manager account. For instructions on how to change "Changing a User Password" on page 55.

Note

Write down the new password and keep it in a safe and secure location. If you forget the manager password, you cannot manage the switch if there are no other management accounts on the unit. In this case, contact Allied Telesis Technical Support for assistance.

For instructions on how to create additional management accounts, see "Adding a New User Account" on page 53.

Assigning a Name to the Switch

The switch is easier to identify if you assign it a name. The switch's name is displayed on the Dashboard page. To change the name of the switch, see "Setting the Switch Information" on page 48.

A name can be up to 39 alphanumeric characters. Special characters, except spaces and quotation marks, are allowed.

Changing a Management IP Address

The switch shipped from the factory has the IP address 169.254.1.1 assigned. You must change the factory default IP address to an address in your network. To change the IP address, see "Changing an IPv4 Address" on page 236. Also, remember to change the IP address of your PC.

Note

When you change the management IP address of the switch, you lose the connection to the switch. After you change the IP address of your PC, start a management session again by opening a web browser on the PC and entering the new IP address of the switch.

Here are the requirements:

- You can assign one IPv4 address per VLAN.
- The switch can have as many IPv4 addresses as there are VLANs on the switch.

- The management IPv4 address can be any IPv4 address assigned on the switch.
- The switch can have only one IPv6 address.
- Your PC must have an IP address that belongs to the network where the management IP address belongs, or have access to the network where the management IP address belongs.

Setting System Time

To set the system time either manually or with an NTP server, see “Setting the System Date and Time” on page 40.

Starting a Web Management Session

This section provides how to start a Web management session when the switch does not have the factory default configuration.

To log on to the switch through the Web interface, enter the IP address of the switch on the Web browser, such as Windows Explorer, on the PC or laptop that can access to the switch. If the AlliedWare Plus™ Web interface comes up, you can skip the rest of this section and continue a Web management session. If the Web interface does not come up, you must configure the switch using the AlliedWare Plus™ Command Line Interface (CLI).

Note

For more information about how to start the Command Line Interface (CLI), see the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User's Guide*.

There are some cases that you must configure the switch using the CLI to start a Web management session:

- ❑ The switch does not have an IP address assigned, or you do not know the IP address of the switch.
- ❑ HTTP service on the switch is disabled.
- ❑ You want to access the switch in the HTTPS mode.

When You Do Not Know the IP Address of the Switch

If the switch has no IP address assigned, or you do not know the IP address of the switch, perform the following steps:

1. “Logging on to the CLI through the Console Port” on page 33.
2. “Checking for the IP Addresses of the Switch in the CLI” on page 34.
3. If the switch does not have any IP address assigned, “Adding an IP Address to the Switch in the CLI” on page 34.
4. “Checking the Status of HTTP and HTTPS Services in the CLI” on page 34.
5. “Enabling HTTP or HTTPS Service in the CLI” on page 35.
6. “Saving your Changes in the CLI” on page 36.

When the Switch Does Not Display the Login Page

When the switch does not display the Web interface even though you enter the IP address of the switch on the Web browser, you must enable HTTP or HTTPS service on the switch through the CLI by performing the following steps:

1. “Logging on to the CLI through the Console Port” on page 33.

Or

Log on to the CLI using the Telnet or SSH protocol.

Note

To start a Telnet or SSH management session, see *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User's Guide*.

2. “Checking the Status of HTTP and HTTPS Services in the CLI” on page 34.
3. “Enabling HTTP or HTTPS Service in the CLI” on page 35.
4. “Saving your Changes in the CLI” on page 36.

Logging on to the CLI through the Console Port

To log on to the CLI through the console port on the switch, perform the following procedure:

1. Connect the RJ-45 connector on the management cable to the console port on the switch.
2. Connect the other end of the cable to an RS-232 port on a terminal or a PC with a terminal emulator program.
3. Configure the terminal or terminal emulator program as follows:
 - Baud rate: 9600
 - Data bits: 8
 - Parity: None
 - Stop bits: 1
 - Flow control: None
4. Press Enter.

You are prompted for a user name and password.

5. Enter a user name and password. If this is the initial management session of the switch, enter “manager” as the user name and “friend” as the password. The user name and password are case sensitive.

The local management session is started when the AlliedWare Plus™ command line prompt is displayed as shown in Figure 4 on page 34.

```
awplus>
```

Figure 4. AlliedWare Plus™ Command Line Prompt

Checking for the IP Addresses of the Switch in the CLI

To check for IP addresses assigned to the switch, enter the following commands:

```
awplus> enable  
awplus# show ip interface
```

For a display of this command, see Figure 5.

```
awplus# show ip interface  
Interface      IP-Address      Status      Protocol  
  vlan1-0      192.168.1.3/24  admin up    running
```

Figure 5. Displaying the IP Address

Adding an IP Address to the Switch in the CLI

When the switch does not have an IP address, assign an IP address and subnet mask to the switch. The following example assigns the IP address 192.168.1.2 and the subnet mask 24 to VLAN 1:

```
awplus> enable  
awplus# configure terminal  
awplus(config)# interface vlan1  
awplus(config-if)# ip address 192.168.1.2/24  
awplus(config-if)#
```

Checking the Status of HTTP and HTTPS Services in the CLI

To check if HTTP service is enabled, enter the following commands:

```
awplus> enable  
awplus# show ip http
```

Figure 6 on page 35 shows an example of the command output.

```
awplus# show ip http
HTTP server disabled.
```

Figure 6. Displaying the Status of HTTP Service

To check whether HTTPS service is enabled, enter the following commands:

```
awplus> enable
awplus# show ip https
```

Figure 7 shows an example of the command output.

```
HTTPS server enabled. Port: 443
Certificate 1 is active
Issued by: self-signed
Valid from: 5/17/2011 to 5/16/2012
Subject: C=US, ST=California, L=San_Jose, O=Jones_Industries, OU=Sales,
CN=167.214.121.45
Finger print: 3FB9D543 72D8E6F8 2159F35E B634A738
```

Figure 7. Displaying the Status of HTTPS Service

Note

HTTPS and HTTP services cannot be enabled at the same time. For example, when HTTP is enabled, HTTPS is disabled.

Enabling HTTP or HTTPS Service in the CLI

To enable HTTP service on the switch, enter the following commands:

```
awplus# configure terminal
awplus(config)# service http
awplus(config)# exit
awplus#
```

To enable HTTPS, the switch must have a certificate. To configure the web server in the HTTPS mode, see the “Secure HTTPS Web Browser Server” chapter in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*.

**Saving your
Changes in the**

CLI

Save your changes to the startup configuration file by entering the following commands:

`awplus# copy running-config startup-config`

Or

`awplus# write`

Saving Your Changes

The changes you have made are temporarily stored in the running configuration file. When you reboot the switch, the information in the running configuration file is lost. To save your changes after you reboot the switch, do the following:

1. Click **SAVE**.

Figure 8 shows the **SAVE** at the upper right corner of the Web page. Clicking **SAVE** saves the changes to the startup configuration file.

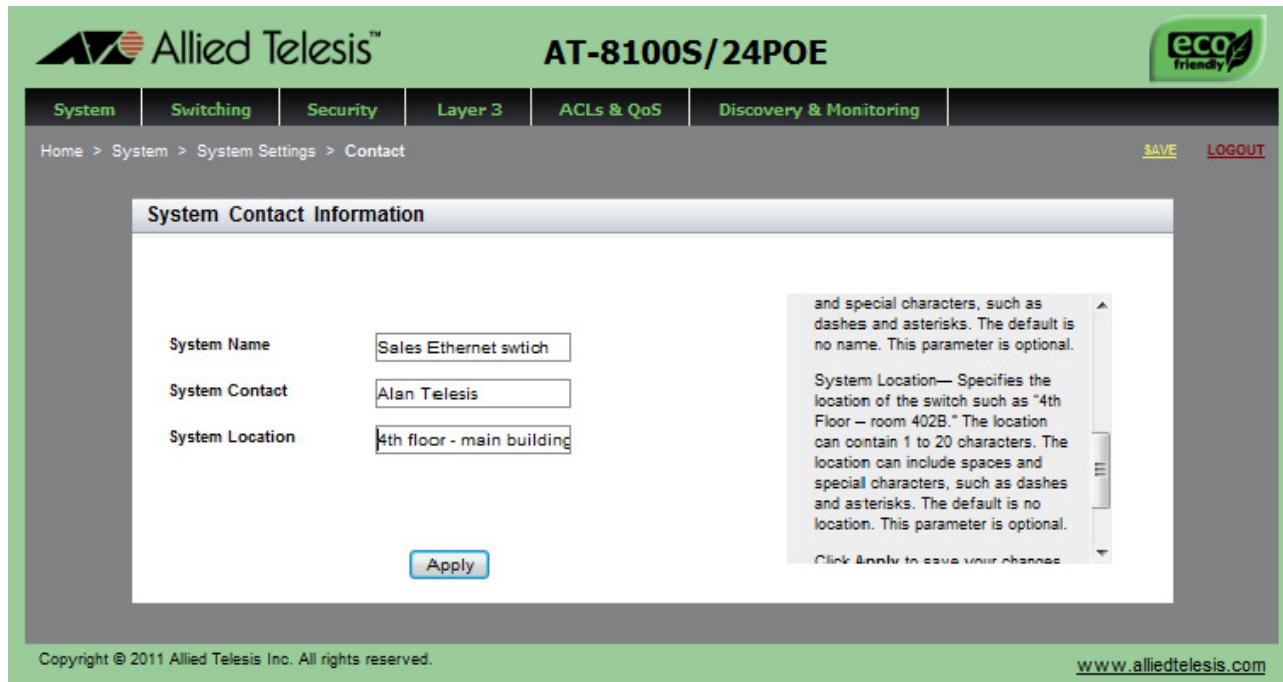


Figure 8. System Contact Information Page

Ending a Web Management Session

To end a web management session, select **LOGOUT** at the top of the web page. For an example, see the System Contact Information page in Figure 8 on page 37.

Chapter 3

Basic Switch Parameters

This chapter describes how to set up basic switch operations in the web interface. See the following sections:

- “Setting the System Date and Time” on page 40
- “Configuring a Telnet or SSH Server” on page 45
- “Configuring a Remote Log Server” on page 47
- “Setting the Switch Information” on page 48
- “Managing the Configuration File” on page 50
- “Managing Local User Accounts” on page 53
- “Rebooting a Switch” on page 59
- “Upgrading the Software” on page 60
- “Returning the AlliedWare Plus Management Software to the Factory Default Values” on page 63
- “Displaying System Information” on page 64

For additional information about basic port settings, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Basic Switch Management
- Basic Switch Management Commands

Setting the System Date and Time

This procedure explains how to set the switch's date and time. Setting the date and time is important if you plan to view the events in the switch's event log or send events to a syslog server. The correct date and time are also important if the management software sends traps to a management workstation or if you plan to create a self-signed SSL certificate. Events, traps, and self-signed certificates should contain the date and time of when they occurred or, in the case of certificates, when they were created.

There are two ways to set the switch's date and time. One method is to set it manually. This method is not recommended because the date and time are lost if you reboot the switch.

The second method uses the Simple Network Time Protocol (SNTP). The AlliedWare Plus Management Software comes with the client version of this protocol. You can configure the AlliedWare Plus™ software to obtain the current date and time from a Network Time Protocol (NTP) or SNTP server located on your network or the Internet.

SNTP is a simplified version of the NTP and uses the same packet structure as NTP uses. The SNTP client software in the AlliedWare Plus™ Management Software is interoperable with NTP servers.

Note

In order for the management software on the switch to communicate with an SNTP or NTP server, there must be an interface on the local subnet from where the switch is reaching the server. The switch uses the IP address of the interface as its source address when sending packets to the server.

Note

The default system time on the switch is midnight, January 1, 2000.

Choose from the following procedures:

- “Configuring an SNTP or NTP Server” on page 40
- “Setting System Time Manually” on page 42

Configuring an SNTP or NTP Server

To configure SNTP or NTP server, do the following:

1. Select the **System** tab.
2. From the System tab, select **System Settings**.

The System Settings Tab is displayed in Figure 9.



Figure 9. System Settings Tab

3. From the System tab, select **System Settings**.
4. Move the cursor to the right and select **Time**.

The System Time Settings page is displayed. See Figure 10.

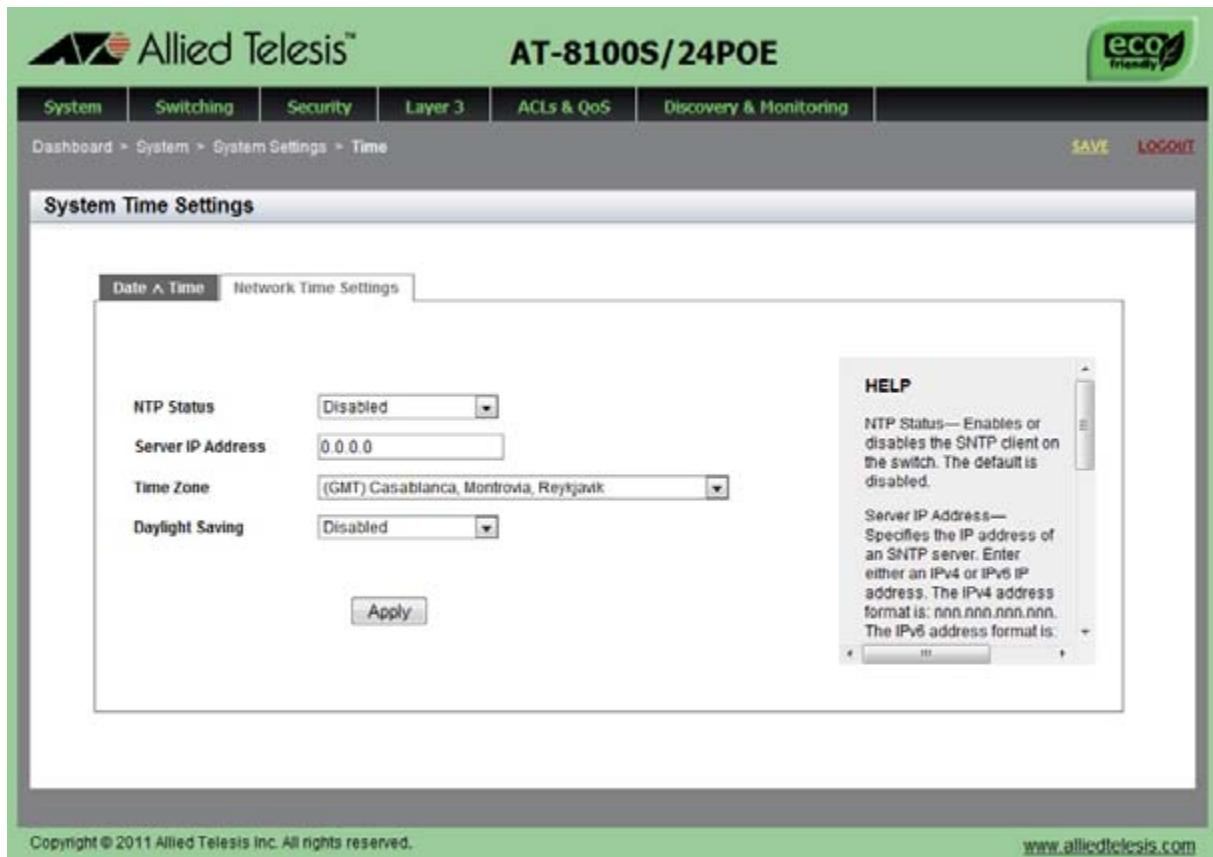


Figure 10. System Time Settings Page with Network Time Settings Tab

5. To configure the switch to obtain its date and time from an SNTP or NTP server on your network or the Internet, specify the following fields:
 - NTP Status**—Select Enabled or Disabled to configure the SNTP client on the switch. The default is disabled.

- Server IP Address**— Specify the IPv4 address of an SNTP or NTP server.

The IPv4 format is: xxx.xxx.xxx.xxx where x is a decimal number from 0 to 255.

Note

If the local interface on the switch is obtaining its IP address and subnet mask from a DHCP server, you can configure the server to provide the interface with an IP address of an NTP or SNTP server. If you configured the server to provide this address, then you do not need to enter it here.

- Time Zone**— Select the time zone as a measurement of Greenwich Mean Time (GMT) which is the default setting. Use the pull-down menu to select the other time zones.
- Daylight Saving**— Enable or disable the system's adjustment for daylight savings time. The default is disabled.

Note

The switch does not set daylight saving time (DST) automatically. If the switch is in a locale that uses DST, you must remember to enable this in March when DST begins and disable it in October when DST ends. If the switch is in a locale that does not use DST, this option should be set to disabled all the time.

6. Click **Apply**.

If you enabled the SNTP client, the switch immediately polls the SNTP or SNTP server for the current date and time. (When SNTP is enabled, the switch automatically polls the server whenever a change is made to any of the fields on this page.)

7. Click **SAVE** to save your changes to the startup configuration file.

Setting System Time Manually

To set the system time manually, do the following:

1. Select the **System** tab.
2. From the System tab, select **System Settings**.

The System Settings Tab is displayed in Figure 9 on page 41.

3. Move the cursor to the right and select **Time**.

The System Time Settings page is displayed. See Figure 10 on page 41.

4. Select the Date & Time tab.

The System Time Settings page with the Date & Time tab is displayed. See Figure 11.

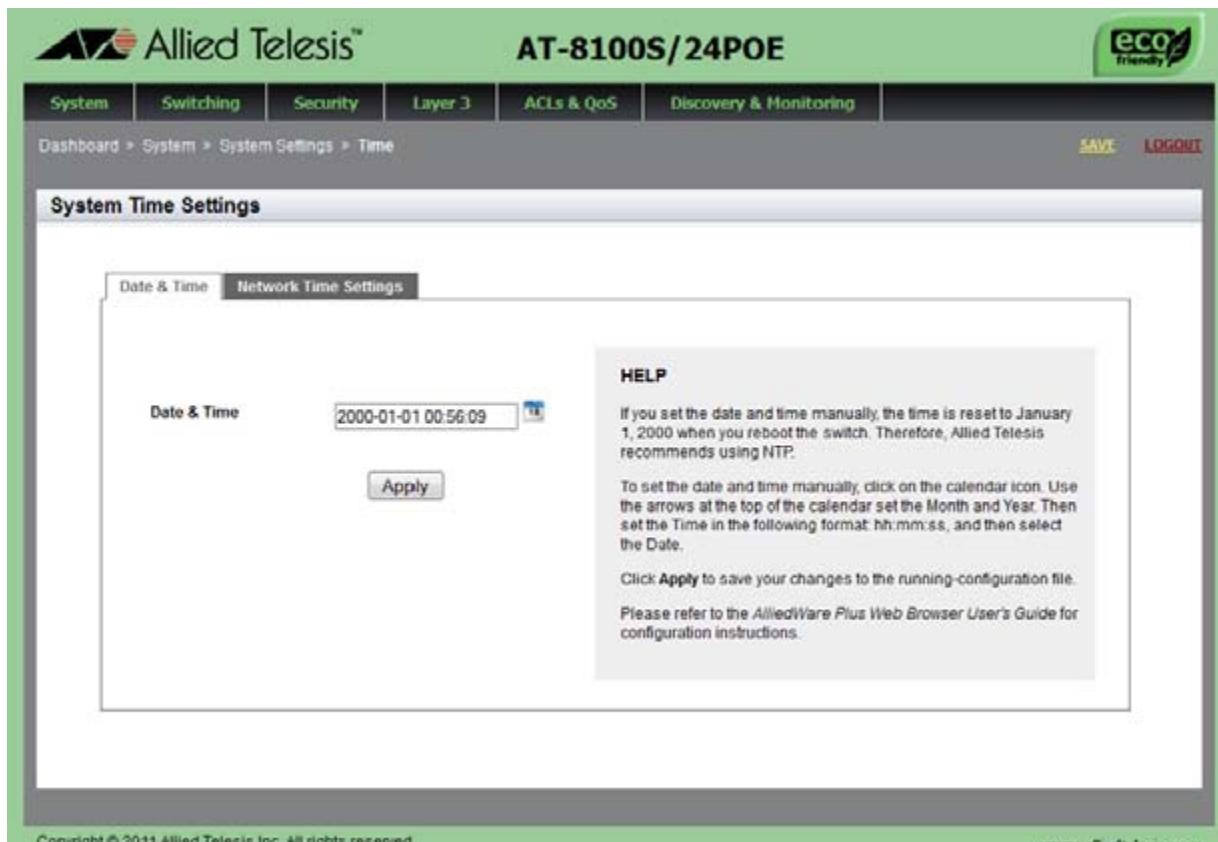


Figure 11. System Time Settings Page with Date & Time Tab

5. You have two ways to set the date and time in the **Date & Time** field. Use either step 6 or 7.
6. Type in the time and date in the following format:
yyyy-dd-mm hh:mm:ss
7. Select the calendar icon next to the **Date & Time** field.

The Calendar page is displayed. See Figure 12 on page 44.



Figure 12. Calendar Page

- a. Use the arrows at the top of the Calendar to select the month and year.
- b. Set the time of day using the following format:
hh:mm:ss
- c. Click on the day of the month.

8. Click **Apply**.

9. Click **SAVE** to save your changes to the startup configuration file.

Configuring a Telnet or SSH Server

The AlliedWare Plus Web Browser interface allows you to configure the switch as a Telnet or SSH server.

You can use the web browser interface to enable a Telnet server, but not as a Telnet client. The Telnet client is only supported from the CLI. For information about how to use a Telnet client, see the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User's Guide*.

To enable an SSH server in the Web interface, you must first create an encryption key in the CLI interface. Then you can enable the SSH server in the web interface.

To assign the switch to a Telnet or SSH server, do the following:

1. From the home page, select the **System** tab.

The System Settings tab is displayed. See Figure 9 on page 41.

2. From the System Settings tab, select **Services**.

The System Services page is displayed. See Figure 13.



Figure 13. System Services Page

3. Specify the following fields as necessary:

- Telnet**— Check the checkbox to enable the Telnet server on the switch. To disable the server on the switch, uncheck the checkbox.
- SSH**— Check the checkbox to enable the SSH server on the switch. To disable the server on the switch, uncheck the checkbox.

Note

Both the Remote Log and Server IP Address fields are used only to set a remote log server. For information on these fields, see “Configuring a Remote Log Server” on page 47.

- Remote Log**— Check the checkbox to enable the switch to send status and error messages to a remote log server. To disable the switch to sent messages to a remote log server, uncheck the checkbox.
- Server IP Address**— Enter the IPv4 address of the remote log server if you check the Remote Log checkbox above. Enter the IP address in the IPv4 format: nnn.nnn.nnn.nnn.

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Configuring a Remote Log Server

You can use the AlliedWare Plus Web browser interface to assign the switch to a remote log server, which is part of the Syslog feature. However, you must use the CLI to view or clear the event log. For information about the Syslog features, see the SysLog chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User's Guide*.

To activate remote logging on the switch, do the following:

1. Select the **System** tab.

The System Settings tab is displayed. See Figure 9 on page 41.

2. From the System Settings tab, select **Services**.

The System Services page is displayed. See Figure 13 on page 45.

3. Specify the following fields:

- Remote Log**— Check the checkbox to enable the switch to send status and error messages to a remote log server. To disable the switch from sending messages to a remote log server, uncheck the checkbox.
- Server IP Address**— Enter the IPv4 address of the remote log server in the IPv4 format: nnn.nnn.nnn.nnn.

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Setting the Switch Information

This procedure allows you to set information about the switch such as a switch name, contact person, and location. Assigning a name to the switch helps you identify your switches when you manage them and help you avoid performing a configuration procedure on the wrong switch.

To assign a name, contact person, and location to the switch, perform the following procedure:

1. From the home page, select the **System tab**.
2. From the System tab, select **System Settings**.

The System Setting tab is displayed. See Figure 9 on page 41.

3. Move the cursor to the right and select **Contact Information**.

The System Contact Information page is displayed. See Figure 14.

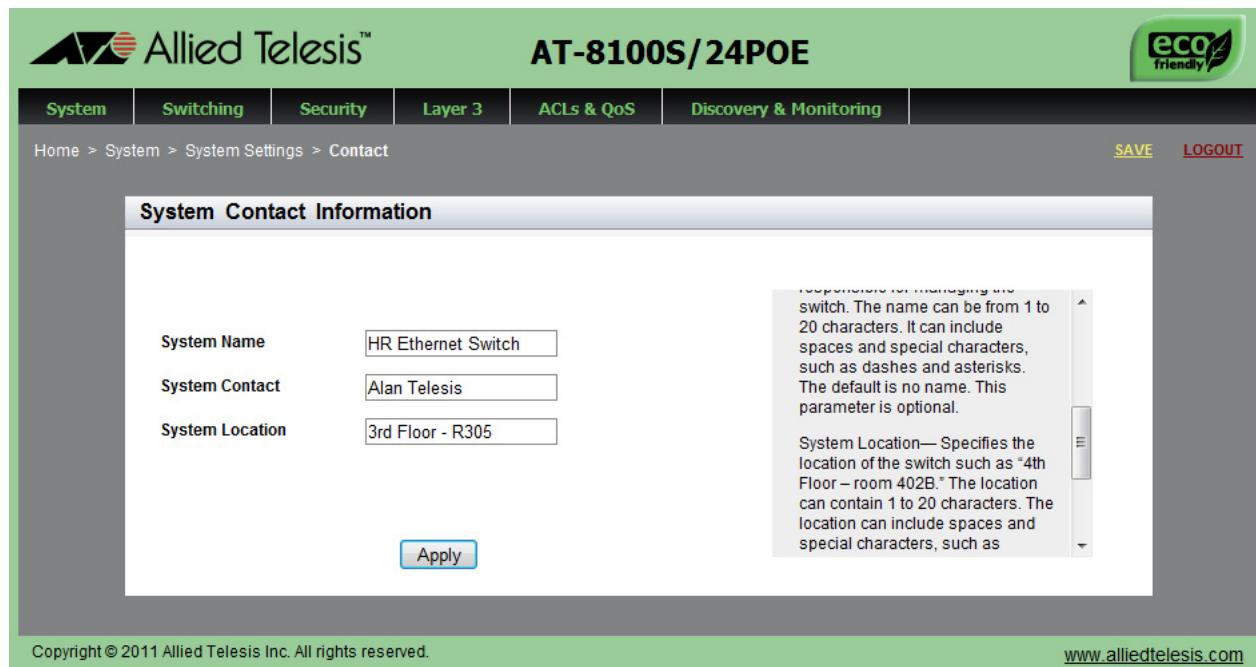


Figure 14. System Contact Information Page

Specify the following fields as necessary:

- System Name**— Enter a name for the switch, for example, S1 or Switch2. The name is displayed on the Dashboard page. See Figure 3 on page 28. The name can be from 1 to 39 characters in length. Special characters, except spaces and quotation marks, are allowed. By default, no system name is specified. This field is optional.
- System Contact** — Enter the name of a network administrator responsible for managing the switch. The name can be from 1 to 255 characters; however, only the first 50 characters are displayed on the Dashboard page. Spaces and special characters, such as dashes and asterisks are allowed. By default, no system contact is specified. This field is optional.
- System Location**— Enter the location of the switch, (for example, 4th Floor - room 402B). The location can be from 1 to 225 characters; however, only the first 50 characters are displayed on the Dashboard page. Spaces and special characters, such as dashes and asterisks are allowed. By default, no system location is specified. This field is optional.

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Managing the Configuration File

Within the web browser interface, you can upload a configuration file on to the switch, download a configuration file from the switch, delete a configuration file, and save your changes to the current configuration file. However, to create a new configuration file, you need to access the switch through the CLI.

See the following procedures:

- “Displaying the Configuration Files” on page 50
- “Setting the Active Configuration File” on page 51
- “Downloading a Configuration File onto Your PC” on page 51

Displaying the Configuration Files

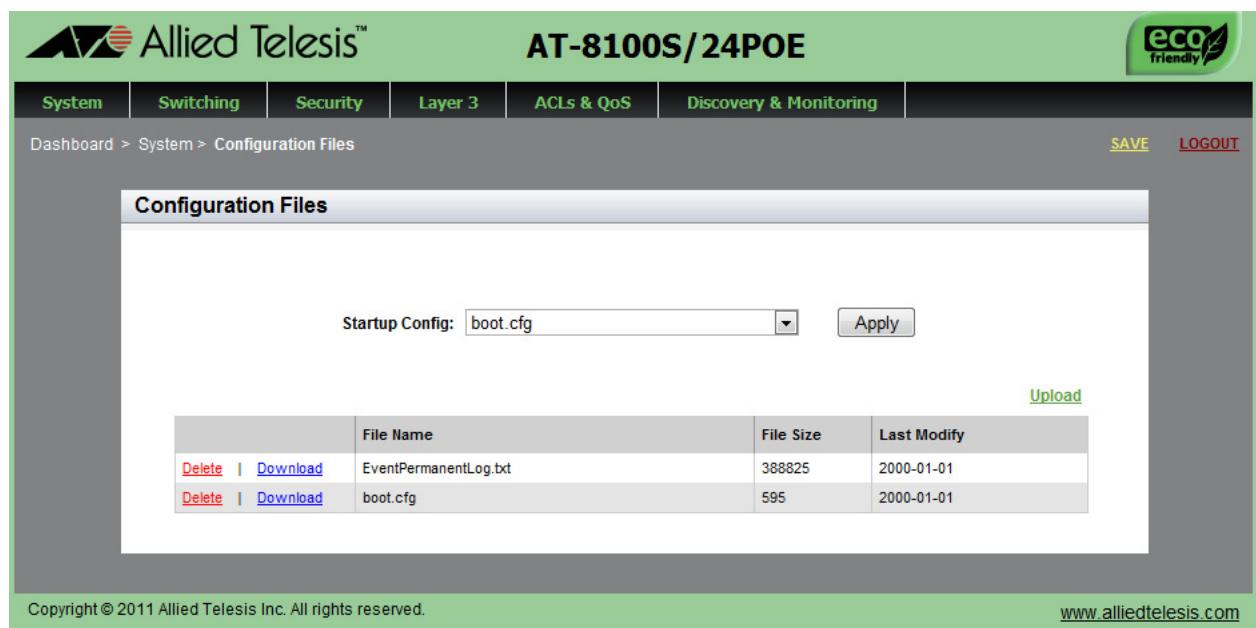
To display a list of the configuration files on the switch, do the following:

1. From the Dashboard page, click the **System** tab.

The System Settings tab is displayed. See Figure 9 on page 41.

2. From the System tab, select **Configuration Files** from the pull-down menu.

For an example of the Configuration Files page, see Figure 15



The screenshot shows the 'Configuration Files' page of the Allied Telesis web interface. At the top, there are tabs for System, Switching, Security, Layer 3, ACLs & QoS, and Discovery & Monitoring. The System tab is selected. Below the tabs, the page title is 'AT-8100S/24POE'. The main content area is titled 'Configuration Files'. It contains a table with two rows of configuration files:

	File Name	File Size	Last Modify
Delete Download	EventPermanentLog.txt	388825	2000-01-01
Delete Download	boot.cfg	595	2000-01-01

At the top of the table, there is a 'Startup Config:' dropdown set to 'boot.cfg' and an 'Apply' button. There is also an 'Upload' link. The bottom of the page includes copyright information and a website link.

Figure 15. Configuration Files Page

The following fields are displayed:

- Startup Config**— Displays the name of the active boot configuration file, which for the switch of the example is “boot.cfg.”
- File Name**— Indicates the name of the configuration file.
- File Size**— Lists the file size in bytes.
- Last Modify**— Indicates the date the configuration file was last modified. The format is year, month, date.

Setting the Active Configuration File

To specify a file as the startup configuration file, do the following:

1. Use the pull-down menu to select a file as the active configuration file.
2. Click **Apply**.

The file you select is the active configuration file after you reboot the switch.

3. Click **SAVE** to save your changes to the startup configuration file.

Downloading a Configuration File onto Your PC

To download a configuration file onto your PC, do the following:

1. Click the **System** tab.

For an example of the System tab, see Figure 9 on page 41.

2. From the System tab, select **Configuration Files**.

For an example of the **Configuration Files** page, See Figure 15 on page 50.

3. Click **Download** next to the file name that you want to download.

For an example of the File Download popup window, see Figure 16.

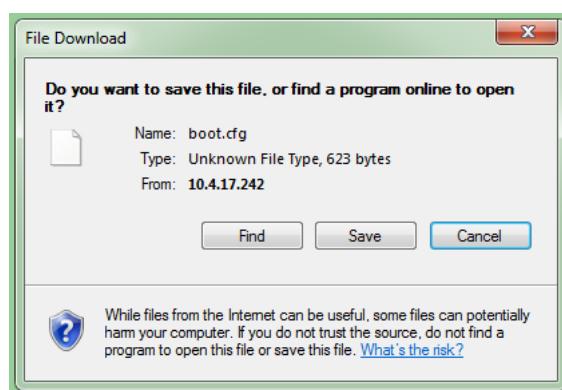


Figure 16. File Download Popup Window of Internet Explorer 8

4. Follow the instructions of your Web browser to select a location and save the file.

Deleting a Configuration

To delete a configuration file, do the following:

1. Click the **System** tab.

For an example of the System tab, see Figure 9 on page 41.

2. From the System tab, select **Configuration Files**.

For an example of the **Configuration Files** page, See Figure 15 on page 50.

3. Click **Delete** next to the file name that you want to download.

The file is deleted.

4. Click **SAVE** to save your changes to the startup configuration file.

Managing Local User Accounts

The switch comes with one local manager account. The account, which has the user name “manager” and default password “friend,” is referred to as a local account because it is the switch that authenticates the user name and password when a manager logs on using the account.

This section explains how to create additional local user accounts, how to change passwords and privileges, and how to delete a manager account. See the following:

- “Adding a New User Account” on page 53
- “Changing a User Password” on page 55
- “Changing the User Privilege” on page 56
- “Deleting a User Account” on page 57

The switch also supports remote manager accounts that are authenticated not by the switch but by a RADIUS or TACACS+ server on your network. For information, see Chapter 17, “RADIUS and TACACS+ Clients” on page 199.

Adding a New User Account

To add a local user account, do the following:

1. From the home page, click the **System** tab.

The System Settings tab is displayed, see Figure 9 on page 41.

2. From the System Settings tab, select **User Management**.

For an example of the User Management page, see Figure 17 on page 54.

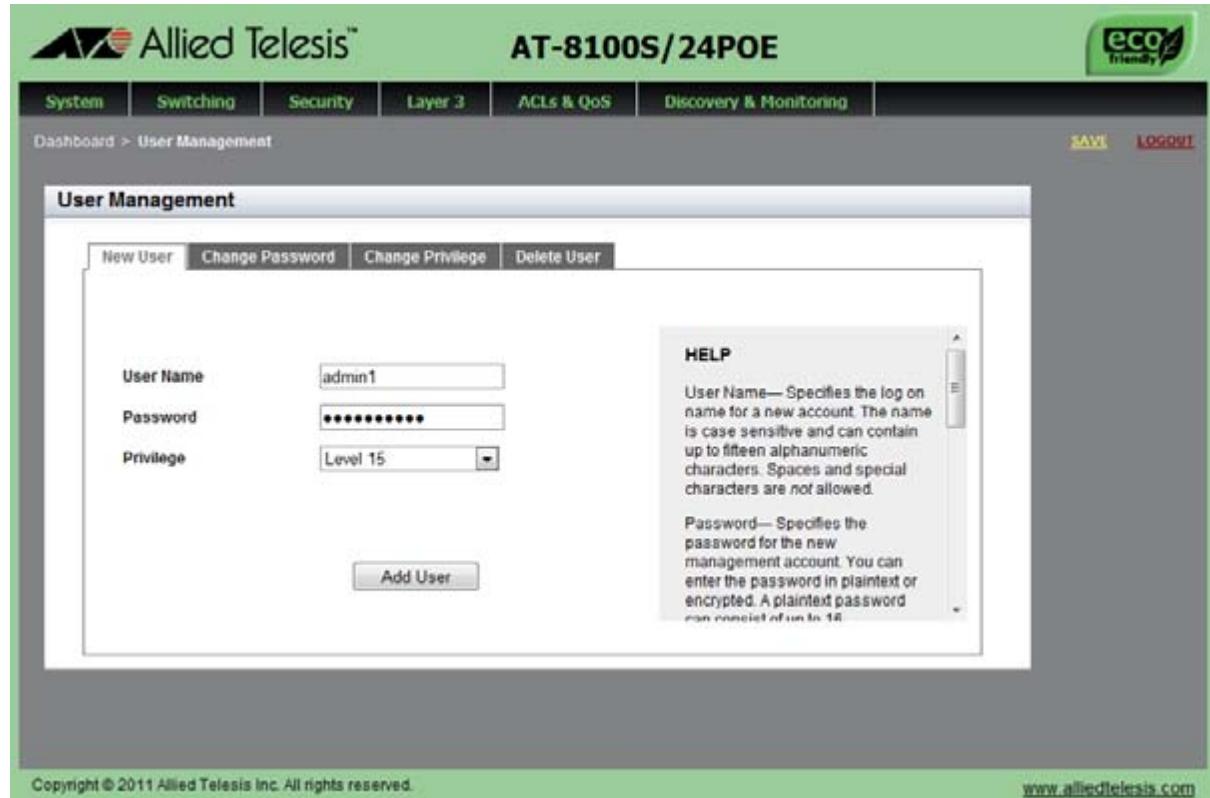


Figure 17. User Management Page

3. Add a new user, do the following:
 - User Name**— Enter a new logon name for the new account. The name is case sensitive and can contain up to 15 alphanumeric characters. Spaces and special characters are *not* allowed.
 - Password**— Enter the password for the new account in plain text. The password can consist of up to 16 alphanumeric characters and is case-sensitive. Spaces and special characters are *not* allowed.
 - Privilege**— Select a user privilege level from the pull-down menu. Choose from the following:
 - Level 15:** Management accounts with a user level of 15 have unrestricted access to the management software. This is the default setting.
 - Level 1:** Management accounts with a user level of 1 have restricted access to the management software. Accounts with this level are allowed to view the settings on the switch, but not allowed to change them.

4. Click **Add User**.
5. Click **SAVE** to save your changes to the startup configuration file.

Changing a User Password

To change a user password, do the following:

1. From the home page, click the **System** tab.
The System Settings Tab is displayed. See Figure 9 on page 41.
2. From the System Settings tab, select **User Management**.
The User Management page is displayed. See Figure 17 on page 54.
3. From the User Management page, select the **Change Password** tab.
The User Management page with the Change Password tab is displayed. See Figure 18.

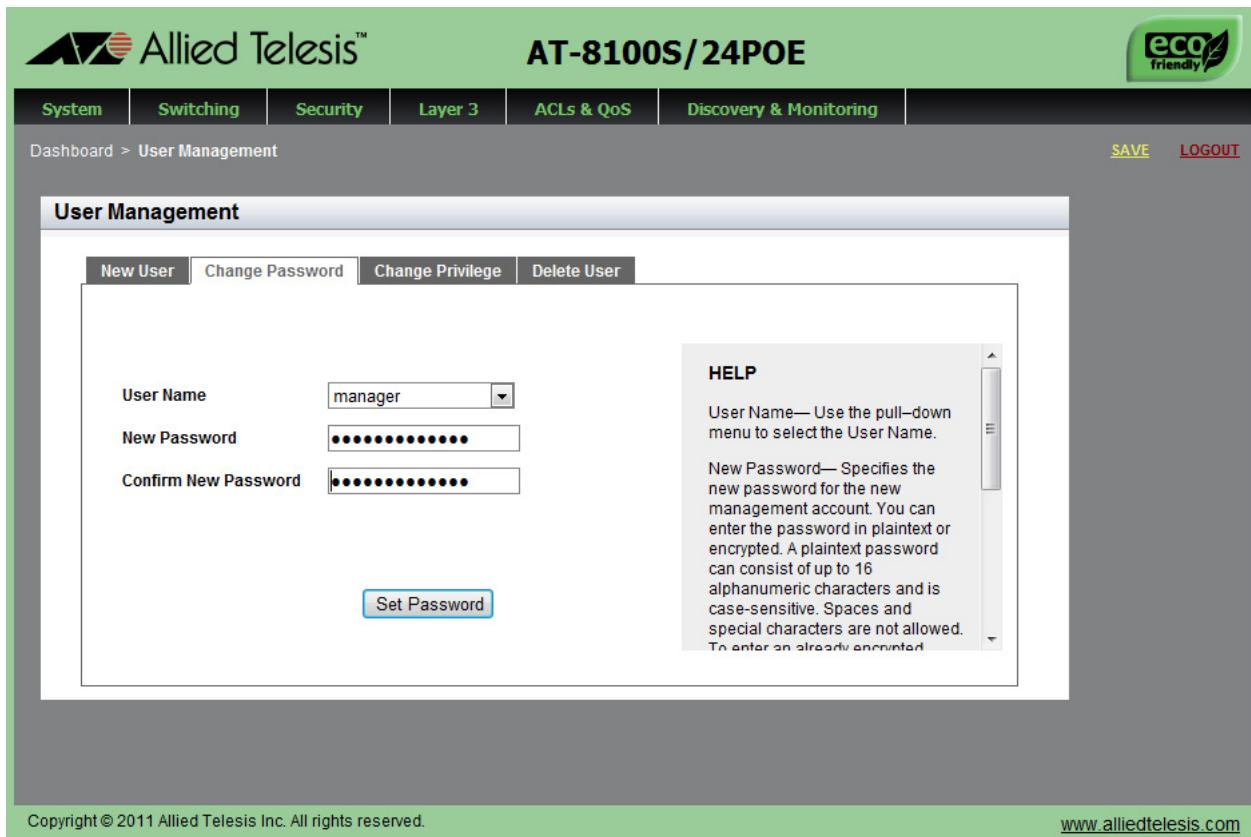


Figure 18. User Management Page with Change Password Tab

4. Use the pull-down menu next to the **User Name** field to select a user name.

The user name must already exist.

5. Enter a new password in plaintext in the **New Password** field.

A password can consist of up to 16 alphanumeric characters and is case-sensitive. Spaces and special characters are *not* allowed.

6. Re-enter the new password in the **Confirm New Password** field.
7. Click **Set Password**.
8. Click **SAVE** to save your changes to the startup configuration file.

Changing the User Privilege

To change a privilege of a user, do the following:

1. From the home page, click the **System** tab.
The System Settings Tab is displayed. See Figure 9 on page 41.
2. From the System Settings tab, select **User Management**.
The User Management page is displayed. See Figure 17 on page 54.
3. From the User Management page, select the **Change Privilege** tab.
The User Management page with the Change Privilege tab is displayed. See Figure 19.

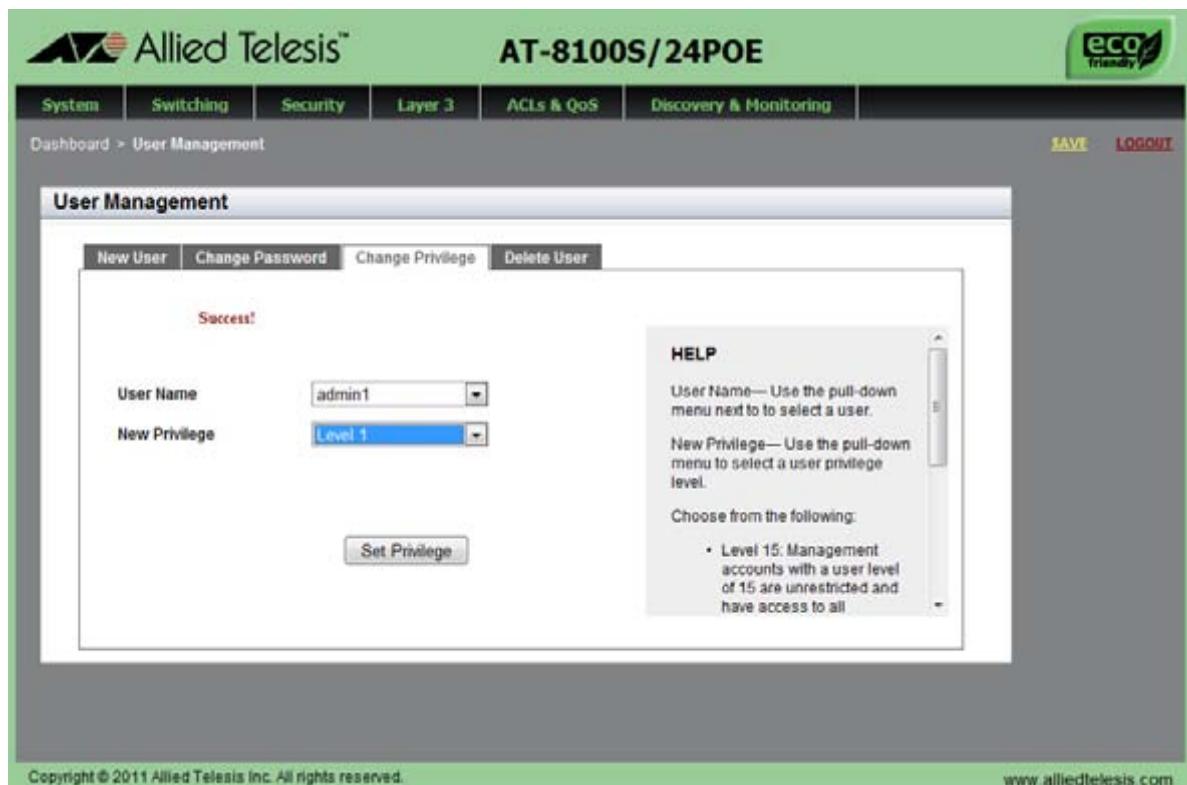


Figure 19. User Management Page with Change Privilege Tab

4. Use the pull-down menu next to the User Name field to select a user.
5. Use the pull-down menu next the New **Privilege** field to select a user privilege level. Choose from the following:
 - Level 15**— Management accounts with a user level of 15 have unrestricted access to the management software.
 - Level 1**— Management accounts with a user level of 1 have restricted access to the management software. Accounts with this level are allowed to view the settings on the switch, but not allowed to change them.
6. Click **Set Privilege**.
7. Click **SAVE** to save your changes to the startup configuration file.

Deleting a User Account

To delete a user account from the switch, do the following:

1. From the home page, click the **System** tab.

The System Settings Tab is displayed. See Figure 9 on page 41.
2. From the System Settings tab, select **User Management**.

The User Management page is displayed. See Figure 17 on page 54.
3. From the User Management page, select the **Delete User** tab.

The User Management page with the Delete User tab is displayed. See Figure 20 on page 58.

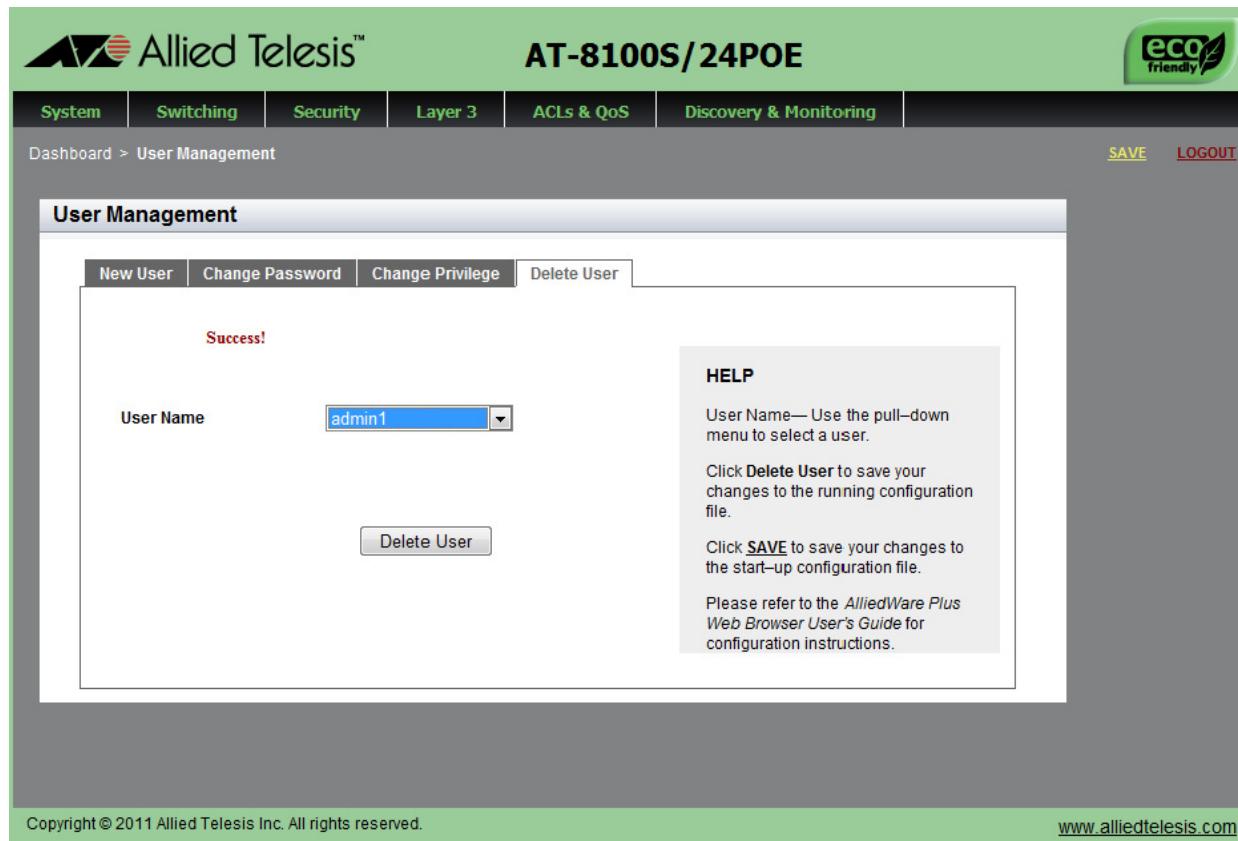


Figure 20. User Management Page with Delete User Tab

4. Use the pull-down menu to select a user.
5. Click **Delete User**.
6. Click **SAVE** to save your changes to the startup configuration file.

Rebooting a Switch

Resetting the switch ends your web browser management session. To continue managing the switch, you must login again.

Note

All unsaved changes are discarded when you reset a switch. To save your changes to the startup configuration file, click **SAVE**.

To reboot a switch, perform the following procedure:

1. Select the **System Tab**.

The System Settings Tab is displayed. See Figure 9 on page 41.

2. From the System Settings tab, select **Dashboard**.

The Dashboard Page is displayed. See Figure 3 on page 28.

3. Select **Reboot** at the bottom of the page.

A confirmation prompt is displayed that indicates that the connection to the web is lost during a reboot.

4. Click **OK** to reset the switch or **Cancel** to cancel the procedure.

Note

The switch does not forward packets while it initializes the AlliedWare Plus™ software and loads its active configuration file. This process takes between 20 seconds to 2 minutes to complete, depending on the number and types of commands in the configuration file.

Upgrading the Software

The latest version of the AlliedWare Plus™ software is available from the Allied Telesis web site. You can download the software image file on your workstation and upload the file onto the switch.

To upgrade the AlliedWare Plus software, perform the following procedure:

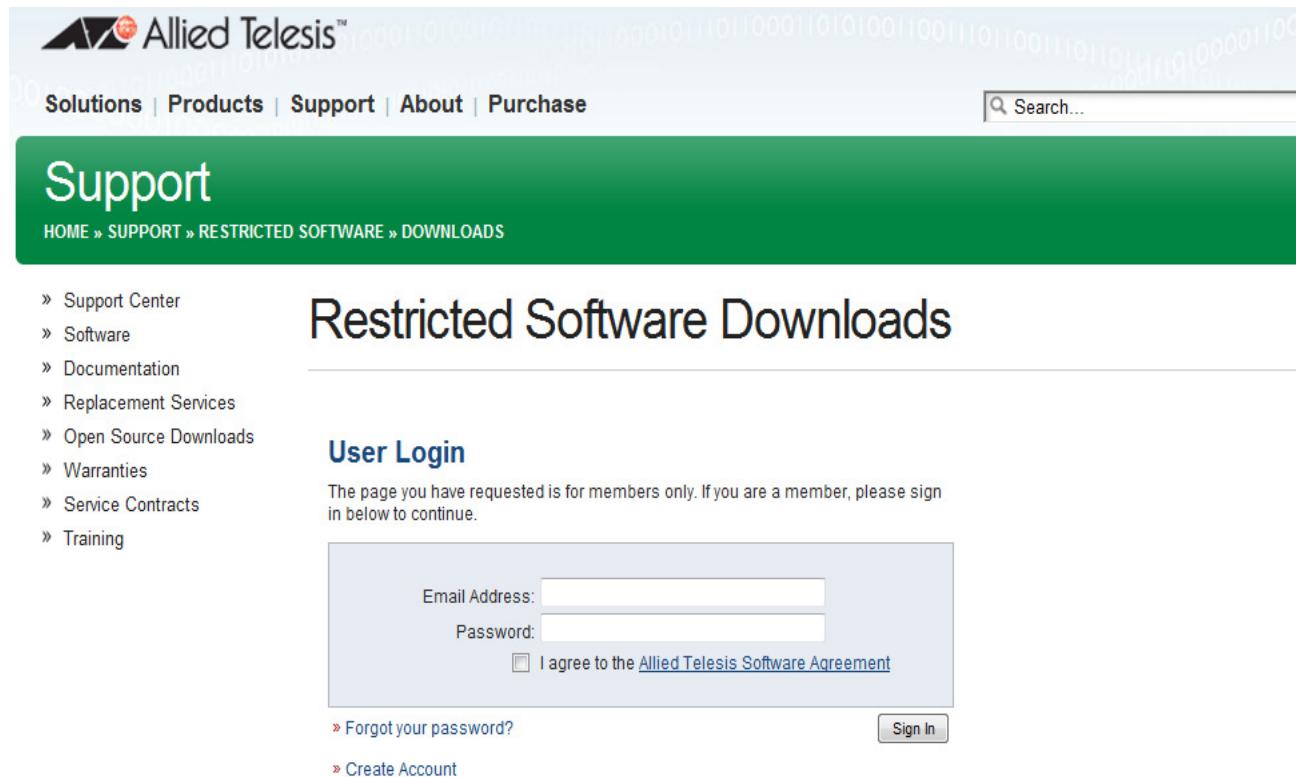
1. Open a new browser and enter the following:

<http://www.alliedtelesis.com/support/software>

The Allied Telesis Software Download page is displayed.

2. Select your hardware product model, such as "AT-8100S/24," from the pull-down menu next to the Product field.
3. Click the software file that you want to upload to the switch.

The User Login page is displayed. See Figure 21.



The screenshot shows the 'User Login' page of the Allied Telesis website. The header includes the logo, navigation links (Solutions, Products, Support, About, Purchase), and a search bar. The main content area has a green header 'Support' and a breadcrumb trail 'HOME > SUPPORT > RESTRICTED SOFTWARE > DOWNLOADS'. On the left, a sidebar lists links: Support Center, Software, Documentation, Replacement Services, Open Source Downloads, Warranties, Service Contracts, and Training. The main content area is titled 'Restricted Software Downloads' and contains a 'User Login' form. The form fields are 'Email Address' and 'Password', with a checkbox for 'I agree to the [Allied Telesis Software Agreement](#)'. Below the form are links for 'Forgot your password?' and 'Create Account', and a 'Sign In' button.

Figure 21. User Login page on the Allied Telesis Website

4. Enter your email address and password, then click the **Sign In** button.

Note

If you do not know your password, click the Create Account link and follow the instructions on the page.

5. Download the software image file to your workstation.
6. Go back to the AT-8100 Web interface and select **Dashboard** from the System Settings tab.

The Dashboard Page is displayed. See Figure 3 on page 28.

Note

All unsaved changes are discarded when you upgrade the software on a switch. To save your changes to the startup configuration file, click **SAVE**.

7. Select **System Upgrade** at the bottom of the page.

The System Upgrade page is displayed. See Figure 22.

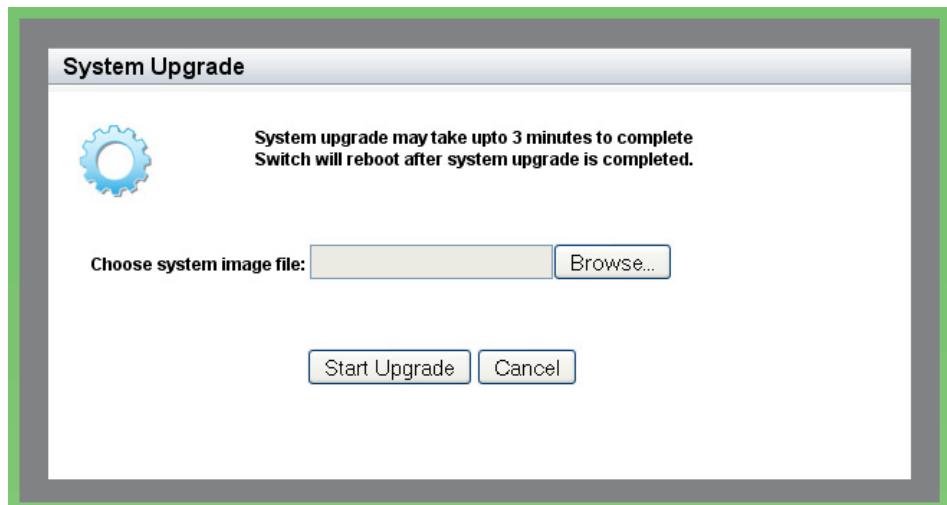


Figure 22. System Upgrade Page

8. Click **Browse** to select an image file.
9. Click **Open** to select the file that you downloaded in step 5.
10. Click **Start Upgrade** to begin the software upgrade or **Cancel** to cancel the procedure.

The upgrade process takes approximately three minutes.

Note

Upgrading the system software on the switch ends your current web browser management session. To continue managing the switch, you must login again.

Returning the AlliedWare Plus Management Software to the Factory Default Values

To reset the AlliedWare Plus Management Software parameters to their default values, you must use the Command Line Interface (CLI). You cannot reset the management software to its factory settings in the web interface. For instructions, see Chapter 7: Basic Switch Management in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User's Guide* on our web site. To locate manuals online, see "Downloading Management Software and Web-based Guides" on page 17.

Displaying System Information

To view basic information about the switch, select the **System** Tab.

The Dashboard Page is displayed as shown in Figure 3 on page 28.

The following fields are displayed:

- Up Time**— Indicates the length of time since the switch was last reset or power cycled in days, hours, minutes and seconds.

The System section displays the following information:

- MAC Address**— Indicates the MAC address of the switch.
- Contact**— Displays the contact person for the switch. To specify this field, see “Setting the Switch Information” on page 48.
- Serial No.**— Displays the unique serial number of the switch.
- Location**— Displays the location of the switch. To specify this field, see “Setting the Switch Information” on page 48.
- System Name**— Indicates the name of the switch. To specify this field, see “Setting the Switch Information” on page 48.
- Version**— Lists the software version number of the AlliedWare Plus software.

The Services section displays the following information:

- IPv6 Management**— Indicates if IPv6 Management is enabled or disabled on the switch.
- Spanning Tree**— Indicates if RSTP or STP is enabled on the switch. The default setting is RSTP.
- 802.1x Port Authentication**— Indicates if 802.1x Port Authentication is enabled or disabled on the switch.
- SNMP**— Indicates the SNMP setting of the switch.
- QoS**— Indicates is QoS is enabled or disabled on the switch.
- RIP**— Indicates the HTTP setting of the switch
- HTTP**— Indicates the HTTP setting of the switch
- LLDP**— Indicates if LLDP is enabled or disabled on the switch.
- Telnet**— Indicates if Telnet is enabled or disabled on the switch.
- SFLOW**— Indicates is sFlow is enabled or disabled on the switch.
- SSH**— Indicates if SSH is enabled or disabled on the switch.
- IGMP Snooping**— Indicates if IGMP Snooping is enabled or disabled on the switch.

- Remote Logging**— Indicates if the remote log is enabled or disabled on the switch.
- IGMP Snooping Querier**— Indicates if IGMP Snooping Querier is enabled or disabled on the switch.

The Administration Options section displays the following information:

- System Upgrade**— Click this link to go to the System Upgrade page to upgrade your system software. See “Upgrading the Software” on page 60.
- Reboot**— Click this link to go to reboot the switch. For instructions, see “Rebooting a Switch” on page 59.

Chapter 4

Setting Port Parameters

This chapter describes how to display and modify the port settings such as back pressure and flow control. In addition, it provides procedures to display and modify storm control settings.

This chapter contains the following sections:

- “Port Numbers on the Switch” on page 68
- “Displaying the Port Parameters” on page 69
- “Changing the Port Settings” on page 72
- “Displaying the Storm Control Settings” on page 76
- “Modifying the Storm Control Settings” on page 78

For additional information about the port parameters and the storm control feature, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Port Parameters
- Port Parameter Commands

Port Numbers on the Switch

The ports on the switch are identified in the format shown in Figure 23.

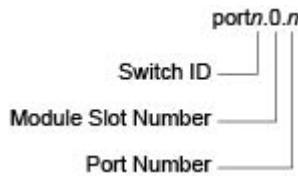


Figure 23. Port Number

The variables in the parameter are defined here:

- Switch ID:** When the switch is a stand-alone switch, the Web interface displays number 1 as the switch ID even though the stand-alone switch displays number 0 on the Stack ID LED. The format of the port for stand-alone AT-8100 Series switches is PORT1.0.<n>.
- When the switch is part of a hardware stack, the Web interface displays the switch ID number that is displayed on the Stack ID LED.
- Module Slot ID:** This number is used to identify a slot in a modular switch. This number should always be 0 for AT-8100 Series switches because they are not modular switches.
- Port number:** This is the port number.

Displaying the Port Parameters

To display the settings for all of the switch ports, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24.

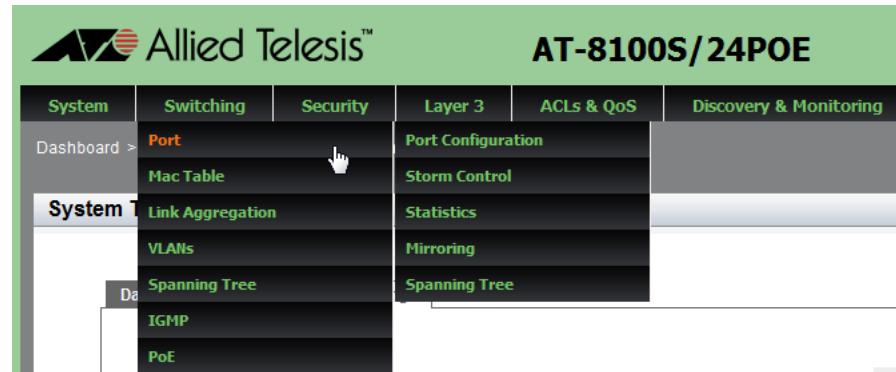


Figure 24. Switching Tab with Port Tab

2. From the Switching tab, select **Port**.

The Port tab expands to the right.

3. From the Port tab, select **Port Configuration**.

The Port Configuration page is displayed. See Figure 25 on page 70.

	Interface	Type	Status	Link	Auto-Neg	Speed	Duplex	Polarity	Back Pressure	Back Pressure Limit	Flow Control	Flow Control Limit	Description
Edit	port1.0.1	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.2	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.3	10/100Base-T	Enabled	Up	Auto	100Mbps	Full	AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.4	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.5	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.6	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.7	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.8	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.9	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.10	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	
Edit	port1.0.11	10/100Base-T	Enabled	Down	Auto			AUTO	Disabled	7935	Disabled	7935	

Figure 25. Port Configuration Page

4. The following fields are displayed:

- Interface**— Indicates the port ID.
- Type**— Indicates the transmission speed and medium, copper or fiber optic, of the port. For example, 1000Base-SX indicates that the port is a fiber optic gigabit standard.
- Status**— Indicates if the port is enabled or disabled. The default setting is “Enabled.” Disabling a port turns off its receiver and transmitter so that the port cannot forward traffic.
- Link**— Indicates the port has successfully connected to a port on another switch or unit.
- Auto-Neg**— Indicates Auto-Negotiation. The setting is “Auto” or “Manual.” The default is “Auto.”
- Speed**— Indicates the speed of the port. The possible options are “10” for 10Mbps, “100” for 100Mbps, and “1000” for 1000Mbps.
- Duplex**— Indicates the duplex mode of the twisted pair port. The setting is “Half” or “Full.”
- Polarity**— Indicates the port’s wiring configuration is MDI (medium dependent interface), MDI-X (medium dependent interface crossover), or the auto setting. This setting only applies to a twisted pair port that is operating at 10 or 100 Mbps.

- Back Pressure**— Indicates if back pressure is enabled or disabled on the port. Back pressure is used by a port during periods of packet congestion to temporarily stop its network counterpart from transmitting more packets. This prevents a buffer overrun and the subsequent loss and retransmission of network packets. A port initiates back pressure by transmitting on the shared link to cause a data collision, which causes its link partner to cease transmission. The default setting is “Disabled.”
- Back Pressure Limit**— Indicates the threshold level for back pressure on the port. Specifies the number of cells for back pressure. The default value is 7935 cells.
- Flow Control**— Indicates if flow control (send and receive) is enabled or disabled on a port. If flow control is enabled, a port sends pause packets when it reaches the point of packet congestion. Also, the port stops transmitting packets when it receives pause packets from its local or remote counterpart. When flow control is disabled, the port sends pause packet regardless of packet congestion. In addition the port continues transmitting packets when it receives pause packets from its local or remote counterpart. The default is “Disabled.”
- Flow Control Limit**— Indicates the threshold level for flow control on a port. The default value is 7935.
- Description**— Indicates the description of a port. To specify this field, see “Changing the Port Settings” on page 72.

Changing the Port Settings

You can change the settings of one port at a time. Use the following procedure to change the port settings or reset a port to its default value,

To change the port settings, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

The Port tab expands to the right.

3. From the Port tab, select **Port Configuration**.

The Port Configuration page is displayed. See Figure 25 on page 70.

4. Click **Edit** next to the port that you want to modify.

The Port Configuration Modify page is displayed. See Figure 26 on page 73.

Port Configuration

HELP

Interface—Indicates the port ID.

Port Type—Indicates the transmission speed and medium that the port supports.

Port Description—Enter a description of 1 to 256 alphanumeric characters for the port. Spaces and special characters are allowed. Note: The description will only show first 30 characters.

Status—Select Enabled or Disabled. The default setting is Enabled. Disabling the port turns off the receiver and transmitter so that the port does not forward traffic.

Negotiation—Select the state of Auto Negotiation on the port. Choose from the following:

- Auto: Enables Auto Negotiation. This is the default setting. When Auto is selected, the Speed and Duplex Mode fields are disabled.

Current Speed: 100Mbps

Current Duplex Mode: Full

Configure Speed: 10Mbps

Configure Duplex Mode: Full

Polarity: AUTO

Back Pressure Status: Disabled

Back Pressure Limit (1-7935): 7935

Flow Control Status: Disabled

Flow Control Limit (1-7935): 7935

Buttons: Apply, Default

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 26. Port Configuration Modify Page

5. Specify the following fields as needed:

- Interface**—Indicates the port ID.
- Port Type**—Indicates the transmission speed and medium, copper or fiber, that the port supports.
- Port Description**—Enter a description of the port. You can enter up to 80 alphanumeric characters; however, only 30 characters are displayed in the Port Configuration List page. Spaces and special characters are allowed.
- Status**—Select either “Enabled” or “Disabled.” The default setting is enabled. Disabling a port turns off its receiver and transmitter so that the port does not forward traffic. You may want to disable a port if there is a problem with a cable or network device.

- Negotiation**— Select the state of Auto Negotiation from the pull-down menu. Setting “Auto” enables Auto Negotiation and setting “Manual” disables Auto Negotiation. The default setting is “Auto.” When the setting for this field is “Auto,” the **Configure Speed** and **Configure Duplex** fields change from white to brown and you cannot select them. To change the **Configure Speed** and **Configure Duplex** fields, change the Negotiation setting to “Manual.”

Note

When the port type is 1000Base fiber optic, the Negotiation must be “Auto” and you are not allowed to change the setting to “Manual.”

- Current Speed**— Displays the current speed of the port.
- Current Duplex Mode**— Displays the current duplex mode setting of the port.
- Configure Speed**— Select a port speed from the pull-down menu. For example, for a 10/100Base-T port, the options are 10 and 100. For a 1000Base-SX/LX port, 1000 is the only option. You can enter a value in this field when the Negotiation is set “Manual.”
- Configure Duplex Mode**— Select the duplex mode of the twisted pair port. Choose from Half, Full, or Auto. A port operating in half-duplex mode can either receive or transmit packets, but not both at the same time. Ports operating in full-duplex can both send and receive packets, simultaneously.
- Polarity**— Select the wiring configuration of the twisted pair port. When a port is operating at 1000 Mbps, the only option is “AUTO.” When operating at 10 or 100 Mbps, in either half- or full-duplex mode, the options are “AUTO,” “MDI,” and “MDI-X.”

To forward traffic, a port on the switch and a port on a network device must have different settings. For instance, the wiring configuration of a switch port has to be MDI if the wiring configuration on a port on a network device is MDIX.

To set the polarity to either “MDI” or “MDI-X” on a port, the Negotiation setting must be “Manual.” A port with the Auto-Negotiation must set the polarity to “AUTO.”

- Back Pressure Status**— Enable or disable back pressure on a port that is operating at 10 or 100 Mbps in half-duplex mode. Back pressure is used by a port during periods of packet congestion to temporarily stop their network counterparts from transmitting more packets. This prevents a buffer overrun and the subsequent loss and retransmission of network packets. A port initiates back pressure by transmitting on the shared link to cause a data collision, which causes its link partner to cease transmission.

To enable and disable back pressure on a port, the speed and duplex mode must be specified manually. You cannot set back pressure on a port that is using Auto-Negotiation.

- Back Pressure Limit (1 - 7935)**— Enter a threshold level for back pressure on the port. Enter the number of cells for back pressure. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.
- Flow Control Status**— Enable or disable the flow control feature. By default, flow control is disabled on the port.
- Flow Control Limit (1 - 7935)**— Set the threshold level for flow control on the port. Enter the number of cells for flow control. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

6. To set the port to the default port value, click **Default**. Otherwise skip this step.
7. Click **Apply**.
8. Click **SAVE** to save your changes to the startup configuration file.

Displaying the Storm Control Settings

To display the storm control settings, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

The Port tab expands to the right.

3. From the Port tab, select **Storm Control**.

The Storm Control List page is displayed. See Figure 27.

	Interface	Broadcast	Broadcast Level	Multicast	Multicast Level	Dif	Dif Level
Edit	port1.0.1	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.2	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.3	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.4	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.5	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.6	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.7	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.8	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.9	Disabled	33554431	Disabled	33554431	Disabled	33554431
Edit	port1.0.10	Disabled	33554431	Disabled	33554431	Disabled	33554431

Figure 27. Storm Control List Page

The following fields are displayed:

- Interface**— Indicates the port ID.
- Broadcast**— Indicates whether the Broadcast threshold setting is enabled or disabled.
- Broadcast Level**— Indicates the maximum number of ingress packets per second of broadcast packets the port receives. Broadcast packets that exceed the threshold are discarded by the port. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.

- Multicast**— Indicates whether the Multicast threshold setting is enabled or disabled.
- Multicast Level**— Indicates the maximum number of ingress packets per second of multicast packets the port receives. Multicast packets that exceed the threshold are discarded by the port. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
- Dlf**— Indicates whether the unknown unicast threshold setting is enabled or disabled.
- Dlf Level**— Indicates the maximum number of ingress packets per second of unknown unicast packets the port receives. Unknown unicast packets that exceed the threshold are discarded by the port. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.

Modifying the Storm Control Settings

To modify the storm control settings, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

The Port tab expands to the right.

3. From the Port tab, select **Storm Control**.

The Storm Control List page is displayed. See Figure 25 on page 70.

4. Click **Edit** on the port that you want to modify.

The Storm Control Settings page is displayed. See Figure 28.

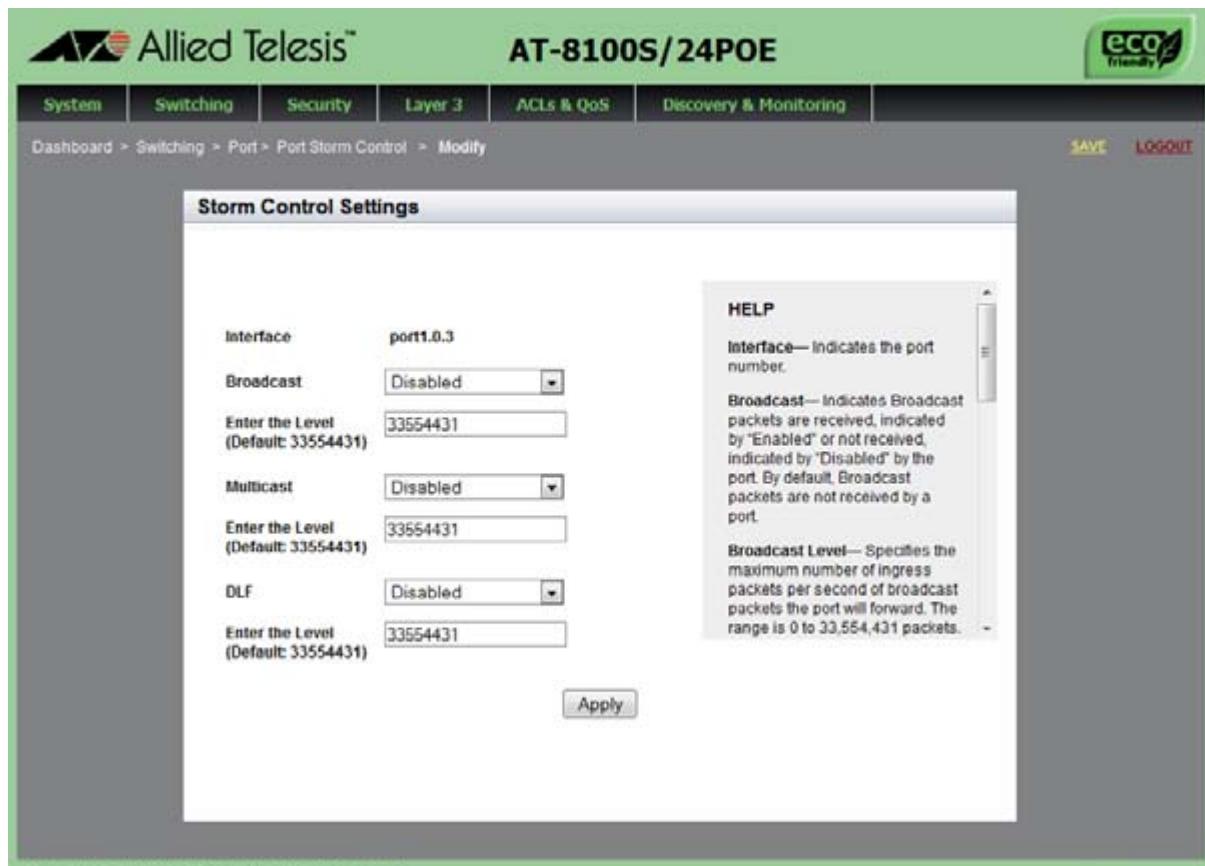


Figure 28. Storm Control Settings Page

5. Change the following fields as needed:

- Broadcast**— Enable or disable the broadcast storm control feature. When this feature is enabled, the port discards ingress packets that exceed the specified level. This feature is disabled by default.
- Enter the Level**— Enter the maximum number of ingress packets per second of broadcast packets the port receives. Broadcast packets that exceed this level are discarded when the feature is enabled. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
- Multicast**— Enable or disable the multicast storm control feature. When this feature is enabled, the port discards ingress packets that exceed the specified level. This feature is disabled by default.
- Enter the Level**— Enter the maximum number of ingress packets per second of multicast packets the port receives. Multicast packets that exceed this level are discarded when this feature is enabled. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.
- DLF**— Enable or disable the unknown unicast storm control feature. When this feature is enabled, the port discards ingress packets that exceed the specified level. This feature is disabled by default.
- Enter the Level**— Enter the maximum number of ingress packets per second of unknown unicast packets the port receives. Unknown unicast packets that exceed this level are discarded when this feature is enabled. The range is 0 to 33,554,431 packets. The default is 33,554,431 packets.

6. Click **Apply**.

7. Click **SAVE** to save your changes to the startup configuration file.

Chapter 5

Setting Port Statistics

This chapter describes how to display and clear port statistics. Within the AlliedWare Plus™ software, you can display and clear transmit, receive, and interface port statistics.

This chapter contains the following topics:

- “Displaying Port Statistics” on page 82
- “Clearing Port Statistics” on page 89
- “Reloading Statistics” on page 90

For additional information about port statistics, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Port Parameters
- Port Parameter Commands

Displaying Port Statistics

You can display several types of port statistics. See the following sections:

- “Displaying Transmit and Receive Port Statistics” on page 82
- “Displaying Receive Statistics” on page 83
- “Displaying Transmit Statistics” on page 85
- “Displaying Interface Statistics” on page 87

Displaying Transmit and Receive Port Statistics

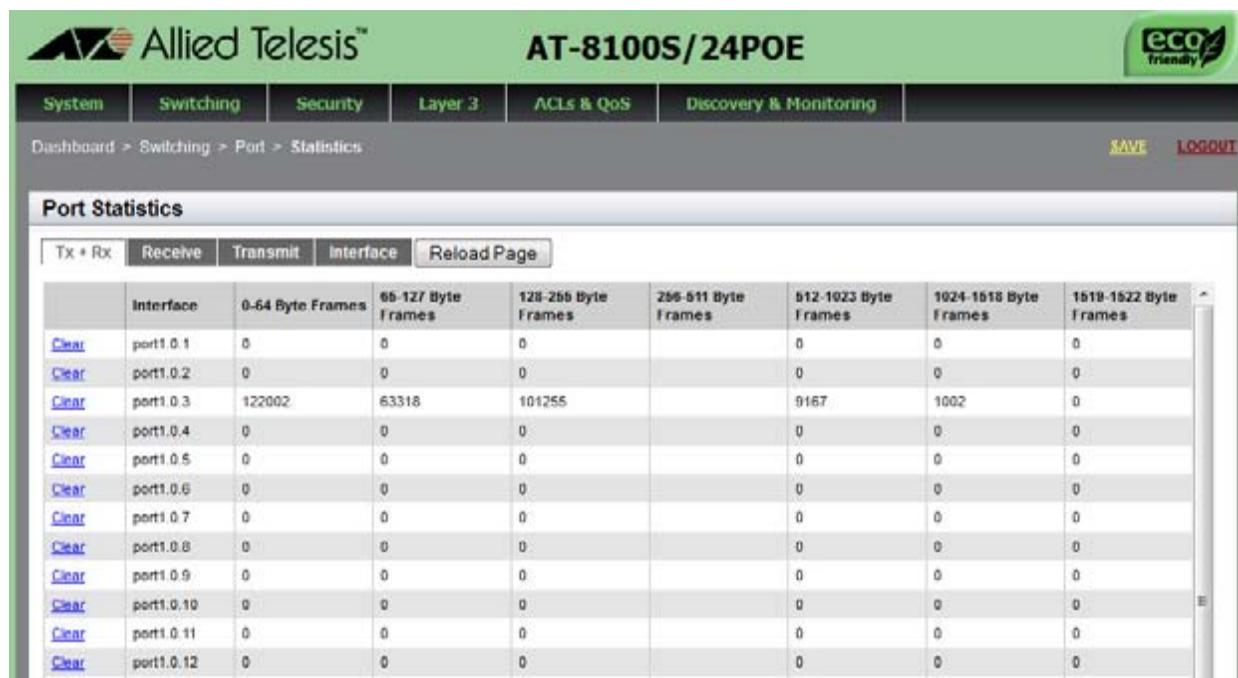
To display the transmit and receive statistics for all of the switch ports, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.
3. Move the cursor to the right and select **Statistics**.

The Port Statistics page is displayed with the Tx + Rx tab automatically selected. See Figure 29.



The screenshot shows the Port Statistics page of the Allied Telesis AT-8100S/24POE web interface. The Tx + Rx tab is selected. The table displays statistics for 12 ports (port1.0.1 to port1.0.12). All values are currently at 0.

	Interface	0-64 Byte Frames	65-127 Byte Frames	128-255 Byte Frames	256-511 Byte Frames	512-1023 Byte Frames	1024-1518 Byte Frames	1519-1522 Byte Frames
Clear	port1.0.1	0	0	0		0	0	0
Clear	port1.0.2	0	0	0		0	0	0
Clear	port1.0.3	122002	63318	101255		9167	1002	0
Clear	port1.0.4	0	0	0		0	0	0
Clear	port1.0.5	0	0	0		0	0	0
Clear	port1.0.6	0	0	0		0	0	0
Clear	port1.0.7	0	0	0		0	0	0
Clear	port1.0.8	0	0	0		0	0	0
Clear	port1.0.9	0	0	0		0	0	0
Clear	port1.0.10	0	0	0		0	0	0
Clear	port1.0.11	0	0	0		0	0	0
Clear	port1.0.12	0	0	0		0	0	0

Figure 29. Port Statistics Page with Tx + Rx Tab

The following fields are displayed:

- Interface**— Indicates the port ID.
- 0-64 Byte Frames**— Indicates the number of frames transmitted by the port that contain 0 to 64 bytes.
- 65-127 Byte Frames**— Indicates the number of frames transmitted by the port that contain 65 to 127 bytes.
- 128-255 Byte Frames**— Indicates the number of frames transmitted by the port that contain 128 to 255 bytes.
- 256-511 Byte Frames**— Indicates the number of frames transmitted by the port that contain 256 to 511 bytes.
- 512-1023 Byte Frames**— Indicates the number of frames transmitted by the port that contain 512 to 1023 bytes.
- 1024-1518 Byte Frames**— Indicates the number of frames transmitted by the port that contain 1024 to 1518 bytes.
- 1519-1522 Byte Frames**— Indicates the number of frames transmitted by the port that contain 1519 to 1522 bytes.

Displaying Receive Statistics

To display the statistics on the Receive Statistics tab, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

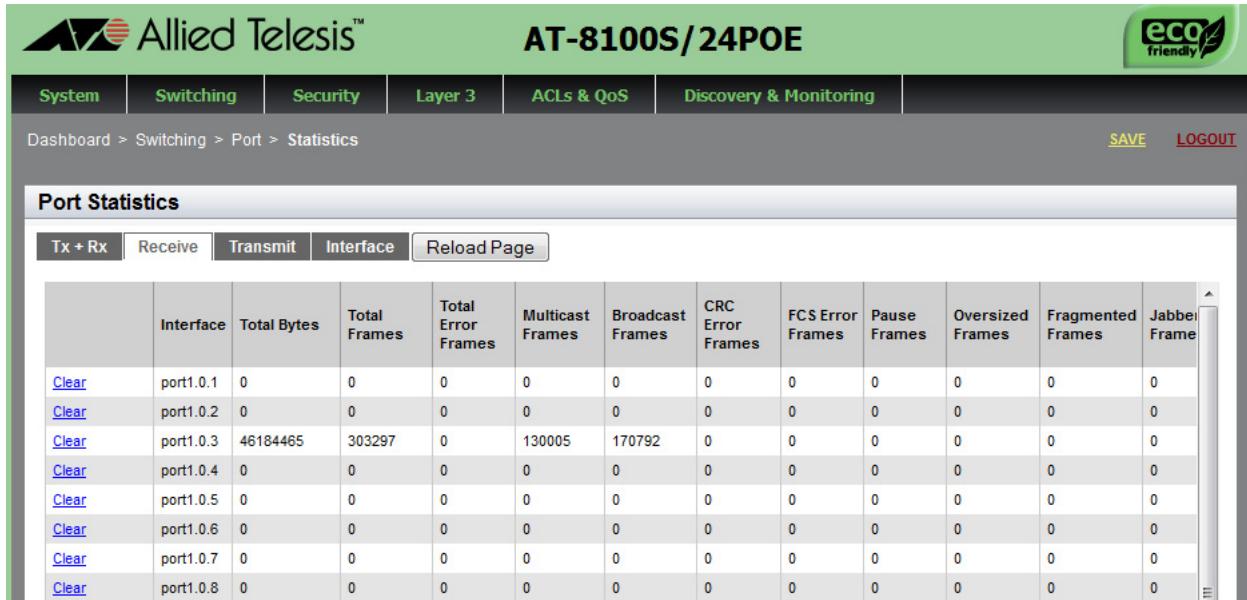
2. From the Switching tab, select **Port**.

3. Move the cursor to the right and select **Statistics**.

The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 29 on page 82.

4. Click on the **Receive** Tab.

The Port Statistics with the Receive tab selected is displayed. See Figure 30 on page 84.



	Interface	Total Bytes	Total Frames	Total Error Frames	Multicast Frames	Broadcast Frames	CRC Error Frames	FCS Error Frames	Pause Frames	Oversized Frames	Fragmented Frames	Jabber Frame
Clear	port1.0.1	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.2	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.3	46184465	303297	0	130005	170792	0	0	0	0	0	0
Clear	port1.0.4	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.5	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.6	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.7	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.8	0	0	0	0	0	0	0	0	0	0	0

Figure 30. Port Statistics with the Receive Tab

The following fields are displayed:

- Interface**— Indicates the port ID.
- Total Bytes**— Indicates the number of received bytes.
- Total Frames**— Indicates the number of received frames.
- Total Error Frames**— Indicates the total number of received frames with errors.
- Multicast Frames**— Indicates the number of received multicast frames.
- Broadcast Frames**— Indicates the number of received broadcast frames.
- CRC Error Frames**— Indicates the number of frames with a cyclic redundancy check (CRC) error but with the proper length (64 - 1518 bytes) received by the port.
- FCS Error Frames**— Indicates the number of ingress frames that had frame check sequence (FCS) errors.
- Pause Frames**— Indicates the number of received flow control pause frames.
- Oversized Frames**— Indicates the number of received frames that exceeded the maximum size as specified by IEEE 802.3 (1518 bytes including the CRC).
- Fragmented Frames**— Indicates the number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors).

- Jabber Frames**— Indicates the number of occurrences of corrupted data or useless signals the port has encountered.

Note

The following fields are not displayed in Figure 30 on page 84.

- Undersize Frames**— Indicates the number of received frames that were less than the minimum length as specified by IEEE 802.3 (64 bytes including the CRC).
- Dropped Frames**— Indicates the number of frames successfully received and buffered by the port, but discarded and not forwarded.
- MTU Exceed Discarded Frames**— Indicates the number of received frames with an MTU that exceeds the MTU of the switch. These frames are discarded.
- MAC Error Frames**— Indicates the number of Receive Error events seen by the receive side of the MAC.

Displaying Transmit Statistics

To display the statistics on the Transmit Statistics tab, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

3. Move the cursor to the right and select **Statistics**.

The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 29 on page 82.

4. Click the **Transmit** tab.

The Port Statistics with the Transmit tab selected is displayed. See Figure 31 on page 86.

The screenshot shows the 'Port Statistics' page of the Allied Telesis AT-8100S/24POE. The 'Interface' tab is selected. The table has 11 columns: Interface, Total Byte, Total Frames, Total Error Frames, Multicast Frames, Broadcast Frames, Pause Frames Sent, Deferred, Single Collision, Multi Collision, Late Collision, and Excessive Collision. The data for each port is as follows:

	Interface	Total Byte	Total Frames	Total Error Frames	Multicast Frames	Broadcast Frames	Pause Frames Sent	Deferred	Single Collision	Multi Collision	Late Collision	Excessive Collision
Clear	port1.0.1	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.2	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.3	1523923	10602	0	9042	0	0	0	0	0	0	0
Clear	port1.0.4	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.5	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.6	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.7	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.8	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.9	0	0	0	0	0	0	0	0	0	0	0
Clear	port1.0.10	0	0	0	0	0	0	0	0	0	0	0

Figure 31. Port Statistics with the Transmit Tab

The following fields are displayed:

- Interface**— Indicates the port ID.
- Total Bytes**— Indicates the number of transmitted bytes.
- Total Frames**— Indicates the number of transmitted frames.
- Total Error Frames**— Indicates the number of transmitted frames with errors.
- Multicast Frames**— Indicates the number of transmitted multicast frames.
- Broadcast Frames**— Indicates the number of transmitted broadcast frames.
- Pause Frames Sent**— Indicates the number of transmitted flow control pause frames.
- Deferred**— Indicates the number of egress frames that the port could not immediately transmit.
- Single Collision**— Indicates the number of frames that were transmitted after at least one collision.
- Multi Collision**— Indicates the number of frames that were transmitted after more than one collision.
- Late Collision**— Indicates the number of late collisions.
- Excessive Collision**— Indicates the number of excessive collisions.

- Total Collision Frames**— Indicates the total number of collisions on the port.
- MAC Error Frames**— Indicates the number of frames not transmitted correctly or dropped due to an internal MAC transmit error.

Displaying Interface Statistics

To display the interface statistics, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

3. Move the cursor to the right and select **Statistics**.

The Port Statistics page with the Tx + Rx tab selected is displayed. See Figure 29 on page 82.

4. Click the **Interface** tab.

The Port Statistics Page with the Interface tab selected is displayed. See Figure 32.

	Interface	Rx Unicast Packets	Rx Discard Packets	Rx IP Header Error Packets	Tx Unicast Packets	Tx Discard Packets	TX Error Packets
Clear	port1.0.1	0	0	0	0	0	0
Clear	port1.0.2	0	0	0	0	0	0
Clear	port1.0.3	2500	109566	0	1560	0	0
Clear	port1.0.4	0	0	0	0	0	0
Clear	port1.0.5	0	0	0	0	0	0
Clear	port1.0.6	0	0	0	0	0	0
Clear	port1.0.7	0	0	0	0	0	0
Clear	port1.0.8	0	0	0	0	0	0
Clear	port1.0.9	0	0	0	0	0	0
Clear	port1.0.10	0	0	0	0	0	0

Figure 32. Port Statistics Page with Interface Tab

The following fields are displayed:

- Interface**— Indicates the port ID.
- Rx Unicast Packets**— Indicates the number of ingress unicast packets.

- Rx Discard Packets**— Indicates the number of ingress packets that were discarded prior to transmission because of an error.
- Rx IP Header Error Packets**— Indicates the number of ingress packets that were discarded because of a hardware error.
- Tx Unicast Packets**— Indicates the number of egress unicast packets.
- Tx Discard Packets**— Indicates the number of egress packets that were discarded prior to transmission because of an error.
- Tx Error Packets**— Indicates the number of egress error packets.

Clearing Port Statistics

To clear the statistics for a port, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

3. Move the cursor to the right and select **Statistics**.

The Port Statistics Page with Tx + Rx tab selected is displayed. See Figure 29 on page 82.

4. Select the desired Port Statistics tab. Choose from the following:

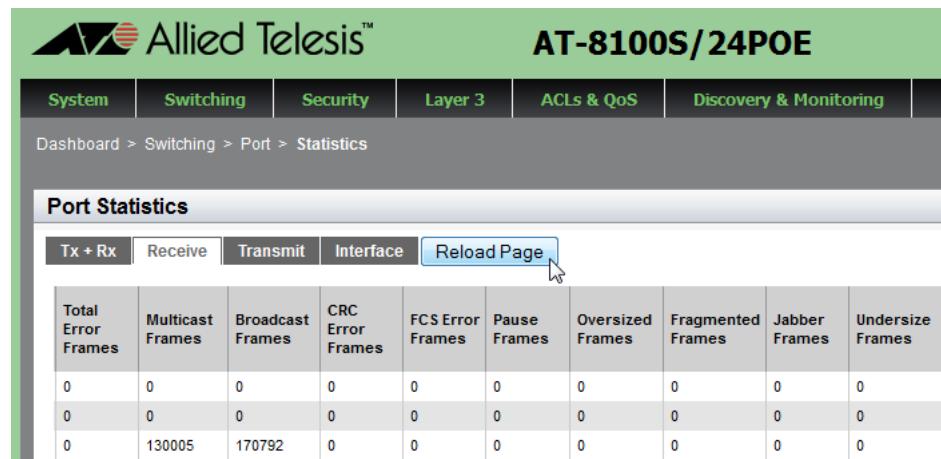
- Tx+Rx**— Displays the transmit and receive statistics.
- Receive**— Displays the receive statistics.
- Transmit**— Displays the transmit statistics.
- Interface**— Displays the interface statistics.

5. Click **Clear** on the port that you want to clear.

Reloading Statistics

Port statistics are constantly counting and the values are changing so that the data that is displayed in the Port Statistics pages is not the most recent. To display the latest data possible, click on the **Reload Page** button on a Port Statistics page.

Figure 33 shows the Reload Page button on Port Statistics page as an example.



The screenshot shows the Port Statistics page for an Allied Telesis AT-8100S/24POE switch. The top navigation bar includes links for System, Switching, Security, Layer 3, ACLs & QoS, and Discovery & Monitoring. The current page is Port Statistics, under the Switching category. The main content area displays a table of port statistics. The table has ten columns: Total Error Frames, Multicast Frames, Broadcast Frames, CRC Error Frames, FCS Error Frames, Pause Frames, Oversized Frames, Fragmented Frames, Jabber Frames, and Undersize Frames. The data in the table is as follows:

Total Error Frames	Multicast Frames	Broadcast Frames	CRC Error Frames	FCS Error Frames	Pause Frames	Oversized Frames	Fragmented Frames	Jabber Frames	Undersize Frames
0	0	0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0	0	0
0	130005	170792	0	0	0	0	0	0	0

Figure 33. Port Statistics Page with the Reload Page Button

Chapter 6

Port Mirroring

The port mirror is a management tool that allows you to monitor the traffic on one or more ports on the switch. It works by copying the traffic from source ports to a destination port where the traffic can be monitored with a network analyzer. The port mirror can be used to troubleshoot network problems or to investigate possible unauthorized network access. The performance and speed of the switch is not affected by the port mirror.

This chapter provides a brief description of the port mirroring feature and explains how to display and set port mirroring. See the following sections:

- “Overview” on page 92
- “Displaying Port Mirroring Settings” on page 93
- “Assigning a Destination Port” on page 95
- “Assigning Source Ports and Port Mirroring Values” on page 96

For more information about port mirroring, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Port Mirror
- Port Mirror Commands

Overview

To use the port mirroring feature, you must designate one or more source ports and one destination port. The source ports are the ports whose packets are mirrored and monitored. The destination port is the port where the packets from the source ports are copied and where the network analyzer is connected. There can be only one destination port on the switch.

Here are guidelines for setting the port mirroring feature:

- The switch supports only one port mirror.
- The port mirror can have one destination port.
- The port mirror can have more than one source port. This allows you to monitor the traffic on multiple ports at the same time. For example, you may monitor the traffic on all the ports of a particular VLAN.
- You can mirror the ingress traffic, the egress traffic, or both on the source ports.
- The destination port must not be a member of a static port trunk or an LACP trunk.

Displaying Port Mirroring Settings

To display the port mirroring assignments for all of the switch ports, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

The Port tab is displayed.

3. From the Port tab, select **Mirroring**.

4. Move the cursor to the right and select **Mirroring**.

The Port Mirroring List page is displayed. See Figure 34.

Interface	Mirror Transmit	Mirror Receive
port1.0.1	X	X
port1.0.2	X	X
port1.0.3	X	X
port1.0.4	X	X
port1.0.5	X	X
port1.0.6	X	X

Figure 34. Port Mirroring List Page

The following fields are displayed:

- **Destination Port**— Use the pull-down menu to select the port where the packets from the source ports are copied and where the network analyzer is connected. You can assign only one destination port to the switch. In Figure 34, the Destination Port is port 1.
- **Interface**— Indicates the port ID.
- **Mirror Transmit**— Indicates a source port whose transmitted, or egress, packets are mirrored and monitored. There can be multiple source ports on the switch.

- **Mirror Receive**— Indicates a source port whose received, or ingress, packets are mirrored and monitored. There can be multiple source ports on the switch.

Assigning a Destination Port

You must assign the destination port before adding source ports. Also, you are allowed to assign only one destination port to the switch.

To assign a destination port, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

The Port tab is displayed.

3. From the Port tab, select **Mirroring**.

The Port Mirroring List page is displayed. See Figure 34 on page 93.

4. Select the pull-down menu next to the **Destination Port** field at the top of the page.

5. Click on the port that you want to designate as the destination port.

You can only assign one destination port to a switch.

6. Click **Apply**.

The **Edit** option is removed from the port. This indicates the destination port for the switch.

7. Click **SAVE** to save your changes to the startup configuration file.

Assigning Source Ports and Port Mirroring Values

To assign mirrored ports and mirroring ports, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

The Port tab is displayed.

3. From the Port tab, select **Mirroring**.

The Port Mirroring List page is displayed. See Figure 34 on page 93.

4. Click Edit next to the port that you want to assign as a transmitting or receiving port mirror.

The Modify Port Mirroring Page is displayed. See Figure 35.

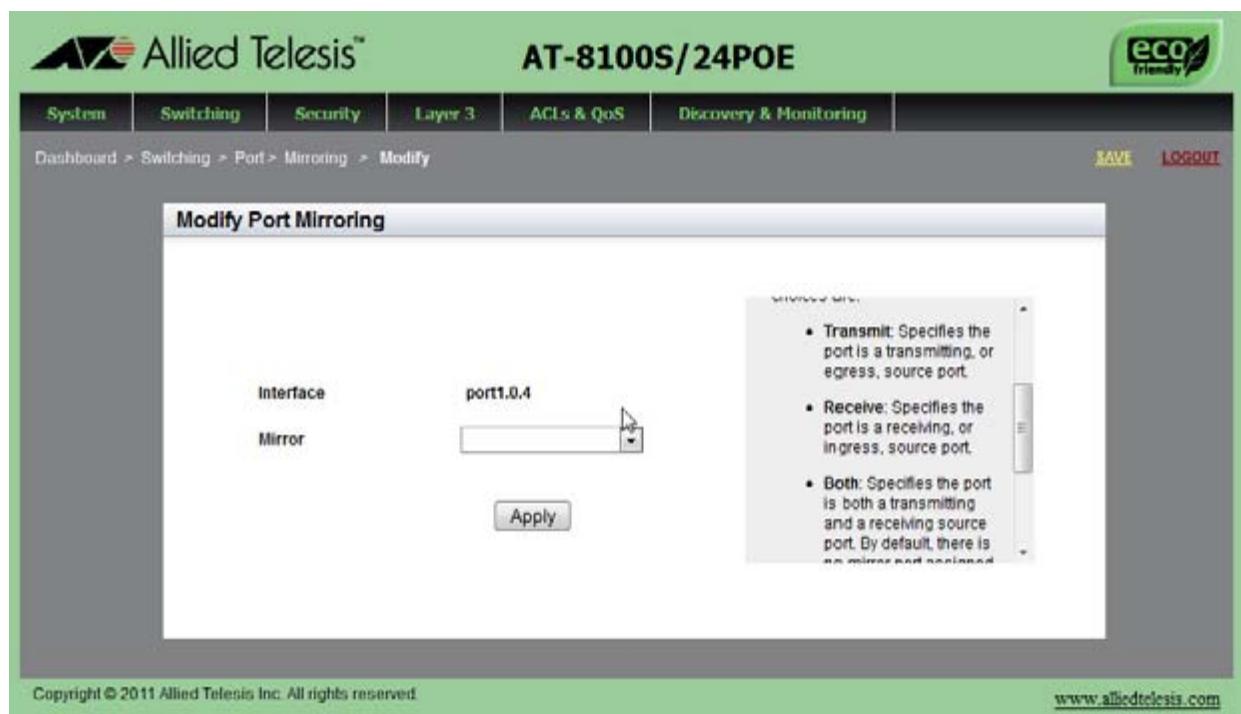


Figure 35. Modify Port Mirroring Page

5. Select the type of mirroring for the port. The options are:

- Transmit**— Specifies the egress traffic on this port to be copied to the destination port.

- Receive**— Specifies the ingress traffic on this port to be copied to the destination port.
- Both**— Specifies both the egress and ingress traffic on this port to be copied to the destination port.

By default, there is no port assigned to port mirroring.

6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Deleting Port Mirroring Settings

You have two ways to delete existing port mirroring settings. When you assign a new port as the destination port, existing port mirroring settings are removed because you can only assign one destination port to the switch. Assigning the port to “None” deletes the existing port mirroring settings as well.

To delete the existing port mirroring settings, assign the port to “None.”

To delete the port mirroring settings, do the following:

1. Display the port mirroring assignments. See “Displaying Port Mirroring Settings” on page 93.

The Port Mirroring List page is displayed. See Figure 34 on page 93.

2. Select the pull-down menu next to the **Destination Port** field at the top of the page.
3. Click on “None.”
4. Click **Apply**.
5. Click **SAVE** to save your changes to the startup configuration file.

Chapter 7

Spanning Tree Protocol on a Port

The Spanning Tree Protocol (STP) and Rapid Spanning Tree Protocol (RSTP) guard against the formation of loops in an Ethernet network topology. A topology has a loop when two or more nodes can transmit packets to each other over more than one data path. Packets can become caught in repeating cycles, referred to as broadcast storms, that AlliedWare Plus™ Version 2.2.4 needlessly consume network bandwidth and that can significantly reduce network performance.

This chapter provides a brief description of the spanning tree protocols and explains how to set spanning tree on a port. See the following sections:

- “Overview” on page 100
- “Displaying Port Spanning Tree Protocol Settings” on page 101
- “Modifying Port Spanning Tree Protocol Settings” on page 103

Note

For information about how to set a spanning tree protocol for the switch, see Chapter 12, “Spanning Tree Protocols on the Switch” on page 153.

For more information about the spanning tree protocols, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Spanning Tree and Rapid Spanning Tree Protocols
- Spanning Tree Protocol (STP)
- STP Commands
- Rapid Spanning Tree Protocol (RSTP)
- RSTP Commands

Overview

STP and RSTP prevent loops from forming by ensuring that only one path is available at a time between the switches in your network. Where multiple paths exist, these spanning tree protocols place the extra paths in a standby or blocking mode. In addition, these protocols can activate redundant paths if primary paths go down. These protocols guard against multiple links between segments and the risk of broadcast storms as well as maintain network connectivity by activating backup redundant paths.

One of the primary differences between the STP and RSTP protocols is in the time each takes to complete the process referred to as convergence. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol determines whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain communications between the various network segments. This is the process of convergence.

With STP, convergence can take up to a minute to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process, and the subsequent loss of data packets. RSTP is much faster than STP. It can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network.

Only one spanning tree can be active on the switch at a time. The default setting is RSTP.

Displaying Port Spanning Tree Protocol Settings

To display the Spanning Tree Protocol settings for all of the switch ports, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

3. Move the cursor to the right and select **Spanning Tree**.

The Port Spanning Tree Settings page is displayed. See Figure 36.

	Interface	Configured Path Cost	Priority	Version	Portfast	Link Type	Loop Guard	Root Guard
Edit	port1.0.1	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.2	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.3	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.4	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.5	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.6	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.7	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.8	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.9	0	128	RSTP	No	AUTO	No	No
Edit	port1.0.10	0	128	RSTP	No	AUTO	No	No

Figure 36. Port Spanning Tree Settings Page

The following fields are displayed:

- Interface**— Indicates the port ID.
- Configured Path Cost**— Indicates the cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1 to 200,000,000.
- Priority**— Indicates a bridge priority number for the switch. The device with the lowest priority number in the spanning tree domain becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

- Version**— Indicates the Spanning Tree Protocol version: STP, RSTP, or MSTP. The default setting is RSTP.
- Portfast**— Indicates if the port is designated as an edge port. If a port on the switch is not connected to a switch or a network that is running the spanning tree protocol, you can designate it as an edge port. A port that is designated as an edge port transitions from blocking to forwarding state immediately to minimize the time that the port must wait for spanning tree to converge.

If an edge port starts to receive BPDUs, the spanning tree protocol no longer considers the port as an edge port.

- Link Type**— Indicates one of the following:
 - Shared:** The shared link type disables rapid transition of the port to the forwarding state during the convergence process. You may want to set link type to shared when the port is connected to a hub with multiple switches connected to it.
 - PTP:** The point-to-point link type allows for rapid transition of the port to the forwarding state during the convergence process.
 - AUTO:** The switch automatically determines the link type of the port.
- Loop Guard**— Indicates the BPDU loop-guard feature on the port is enabled (Yes) or disabled (No). If a port that has this feature activated stops receiving BPDU packets, the switch automatically disables it. A port that has been disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset.

This feature is supported in RSTP and not supported on edge ports. The default setting for BPDU loop-guard on a port is disabled.
- Root Guard**— Indicates if the Root Guard feature is enabled.

Modifying Port Spanning Tree Protocol Settings

To modify port settings for Spanning Tree Protocol, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Port**.

3. Move the cursor to the right and select **Spanning Tree**.

The Port Spanning Tree page is displayed. See Figure 36 on page 101.

4. Click Edit on the port that you want to change.

The Modify Port Spanning Tree Settings page is displayed. See Figure 37.

The screenshot shows the 'Modify Port Spanning Tree Settings' page for port port1.0.3. The page includes the following configuration fields:

- Interface: port1.0.3
- Version: RSTP
- Configured Path Cost (1-200000000): 0
- Priority (0-15) (Actual value is multiple of 16): 8
- Portfast: Disabled
- Link Type: AUTO
- Loop Guard: Disabled
- Root Guard: Disabled

A 'HELP' box provides detailed descriptions for each field:

- Interface**—Indicates the port number.
- Version**—Indicates the Spanning Tree Protocol version. The default is RSTP.
- Configured Path Cost (1-200000000)**—Use this field to specify the cost of a port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1-200000000.

At the bottom of the page, there is an 'Apply' button and a copyright notice: 'Copyright © 2011 Allied Telesis Inc. All rights reserved.' and a website link: 'www.alliedtelesis.com'.

Figure 37. Modify Port Spanning Tree Settings Page

5. Change the following settings as needed:

- Interface**— Indicates the port ID.
- Version**— Indicates the Spanning Tree Protocol version. The default setting is RSTP.
- Configured Path Cost**— Enter the cost of the port to the root bridge. This cost is combined with the costs of the other ports in the path to the root bridge, to determine the total path cost. The lower the numeric value, the higher the priority of the path. The range is 1 to 200,000,000. The default value is 0.
- Priority (0-15)**— Enter the priority value of the port. You can influence which port is elected for a specific port role.

For example, when the switch has the two ports with the same path cost and the path cost is the lowest on the switch, it uses the port priority value to determine which port is the root port.

If both priority values of these two ports are the same, the switch elects a port with the lower port ID.

The range of the priority value is 0 to 240 in increments of 16, for a total of 16 increments. See Table 1. Specify the increment of the desired value. The default port priority is 128 (increment 8).

Table 1. STP Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

- PortFast**— Select “Enabled” to assign the port as an edge port, or “Disabled” to assign the port as a non-edge port. Assign the port as an edge port if the port is not connected to spanning tree devices or to LANs that have spanning tree devices. An edge port transitions from blocking to forwarding state immediately so that the host connected to the edge port can connect to the network immediately rather than waiting for spanning tree to converge.

When an edge port starts to receive BPDUs, the switch no longer considers the port as an edge port.

- Link Type**— Choose from the following settings:

AUTO: The switch determines the link type of the port is either PTP or Shared. If a port is set to full-duplex mode, the link type is point-to-point. If a port is set to half-duplex mode, the link type is shared.

PTP: Allows the port rapid transition to the forwarding state during the convergence process of the spanning tree domain.

Shared: Disables rapid transition. You may want to set the link type to shared if the port is connected to a hub with multiple switches connected to it.

- Loop Guard**— Enable or disable the BPDU loop-guard feature on the port. If a port with the loop guard activated stops receiving BPDU packets, the switch automatically shut down the port. A port that is disabled by the feature remains in that state until it begins to receive BPDU packets again or the switch is reset. The default setting for BPDU loop-guard on the ports is disabled.
- Root Guard**— Enable or disable the Root Guard feature.

6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Chapter 8

Setting the MAC Address

The procedures in this chapter describe how to display the MAC address table that resides on the switch as well as how to add a unicast or multicast MAC addresses to the table. Procedures to modify and delete MAC addresses within the table are also included in this chapter.

See the following sections:

- “Displaying the Unicast MAC Addresses” on page 108
- “Displaying the Multicast MAC Addresses” on page 110
- “Assigning a Unicast MAC Address” on page 111
- “Assigning a Multicast MAC Address” on page 113
- “Deleting a Unicast MAC Address” on page 115
- “Deleting a Multicast MAC Address” on page 116

For more information about MAC addresses, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- MAC Address Table
- MAC Address Table Commands

Displaying the Unicast MAC Addresses

To display the unicast MAC addresses, do the following:

1. Select the Switching Tab.

The Switching Tab is displayed. See Figure 38.

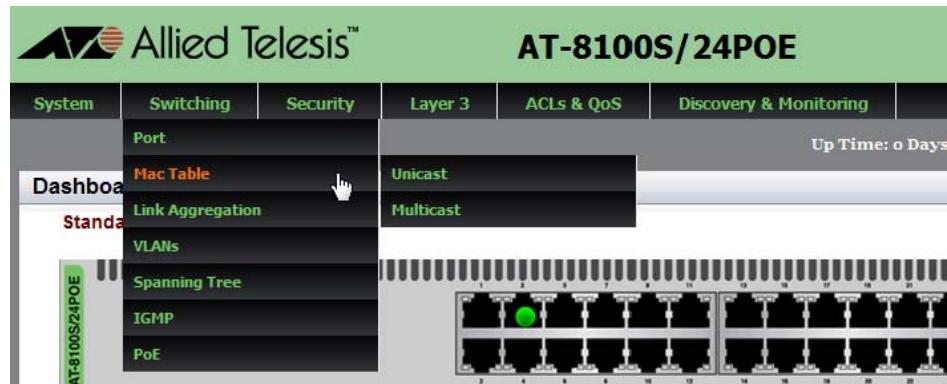


Figure 38. Switching Tab

2. Select **Mac Table** and then move the cursor to the right to select **Unicast**.

The Unicast MACs page is displayed. See Figure 39.

Unicast MACs				
Number of Unicast MACs: 91				
Add Clear Static Clear Dynamic				
	MAC Address	Vlan	Port	Type
Delete	00-00-00-00-02-50	Vlan1	1	dynamic
Delete	00-00-00-00-02-60	Vlan1	1	dynamic
Delete	00-00-CD-14-64-48	Vlan1	1	dynamic
Delete	00-04-5A-5E-6F-D3	Vlan1	1	dynamic
Delete	00-06-58-A3-67-06	Vlan1	1	dynamic
Delete	00-06-58-CB-00-16	Vlan1	1	dynamic

Figure 39. Unicast MACs Page

The following fields are displayed:

- MAC Address**— Indicates the dynamic and static unicast MAC addresses learned on or assigned to the port.
- Vlan**— Indicates the ID number of the VLAN that the node designated by the MAC address belongs to. The default VLAN is Vlan1.
- Port**— Indicates the port number where the address was learned on or assigned to.
- Type**— Indicates the type of MAC address entry, static or dynamic.

Displaying the Multicast MAC Addresses

To display the multicast MAC addresses, do the following:

1. Select the Switching Tab.

The Switching Tab is displayed. See Figure 38 on page 108.

2. Select **Mac Table** and then move the cursor to the right to select **Multicast**.

The Multicast MACs Page is displayed. See Figure 40.

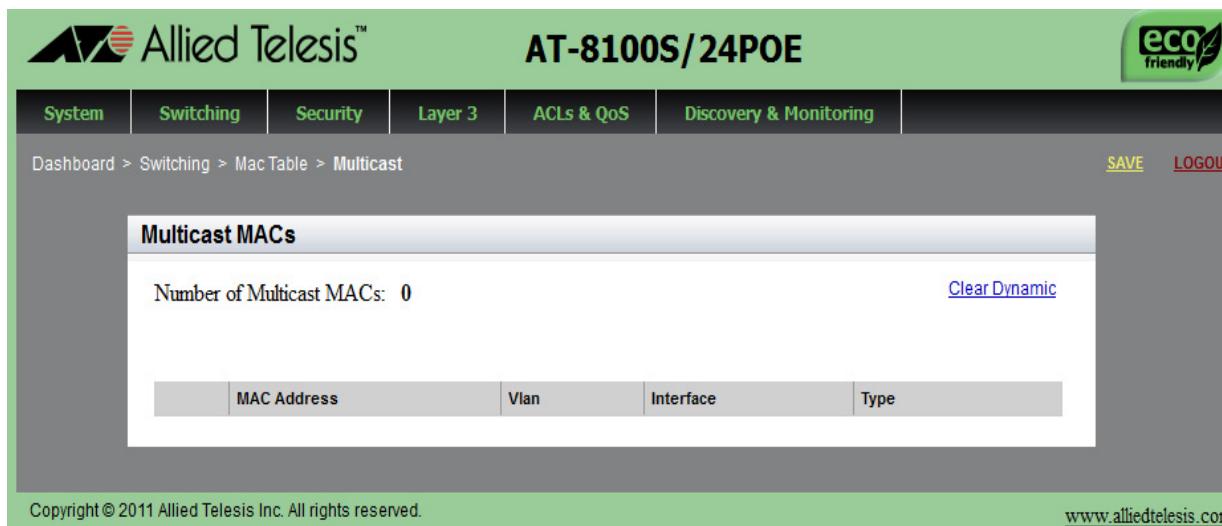


Figure 40. Multicast MACs Page

The following fields are displayed:

- MAC Address**— Indicates the dynamic or static unicast MAC address learned on or assigned to the port.
- Vlan**— Specifies the ID number of the VLAN where the multicast application and the host nodes are members. The default VLAN is Vlan1.
- Interface**— Indicates the port where the address was learned or assigned.
- Type**— Indicates the type of MAC address entry: static or dynamic.

Assigning a Unicast MAC Address

To assign a unicast MAC address to the MAC address table, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. Select **Mac Table** and then move the cursor to the right to select **Unicast**.

The Unicast MACs page is displayed. See Figure 39 on page 108.

3. Click Add.

The Unicast MAC Page is displayed. See Figure 41.

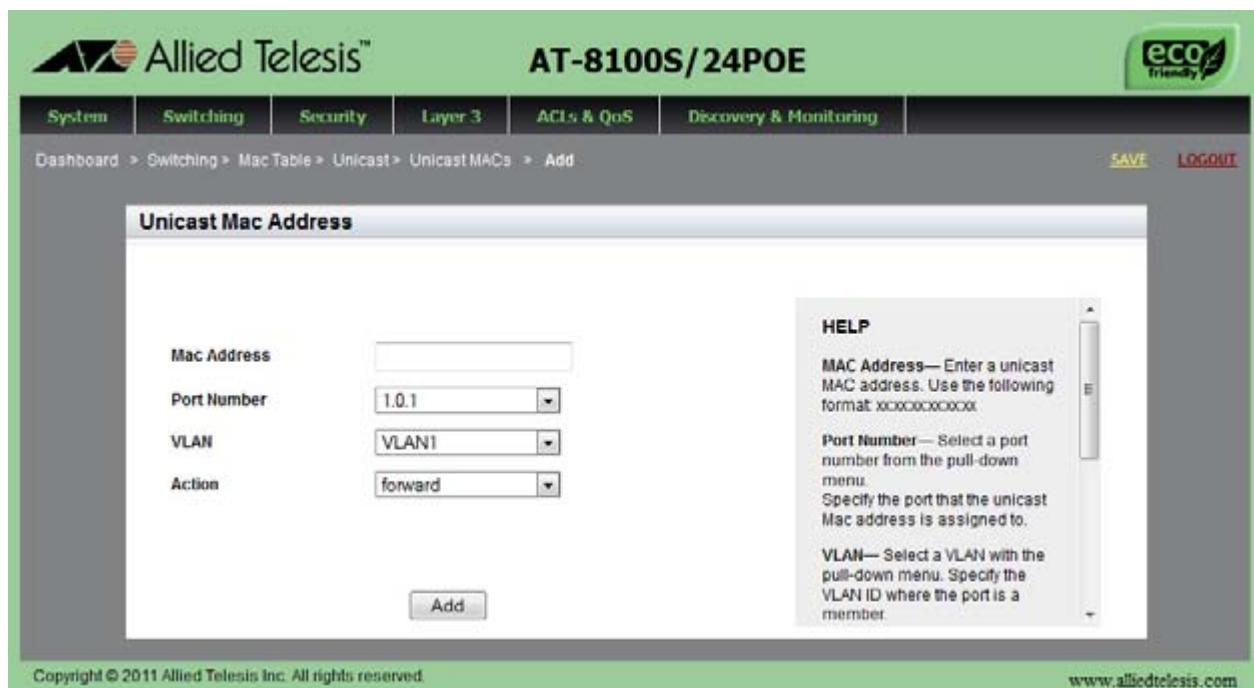


Figure 41. Unicast MAC Address Page

4. Add a new unicast MAC address, do the following:

- MAC Address**— Enter a unicast MAC address. Use the following format:

XX:XX:XX:XX:XX:XX

- Port Number**— Select the port number which the end node of the MAC address is connected.

- VLAN**— Select a VLAN where the port is a member.
- Action**— Select one of the following options:
 - Forward**: Specifies the port to forward packets that have the designated source MAC address.
 - Discard**: Specifies the port to discard packets that have the designated source MAC address.

5. Click **Add**.
6. Click **SAVE** to save your changes to the startup configuration file.

Assigning a Multicast MAC Address

To assign a multicast MAC address to the MAC address table, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. Select **Mac Table** and then move the cursor to the right to select **Multicast**.

The Multicast MACs page is displayed. See Figure 40 on page 110.

3. Click Add.

The Multicast MAC Address page is displayed. See Figure 42.

The screenshot shows the 'Multicast Mac Address' configuration page. The page has the following fields:

- Mac Address:
- Port List:
- Vlan:
- Action:

Below these fields is a 'Add' button. To the right of the fields is a 'HELP' panel with the following text:

Mac Address—Indicates the dynamic or static multicast MAC address learned on or assigned to the port.

Port List—Selects a port list with the Port List pull-down menu. For a multicast address, you can assign more than one port number. Enter multiple ports separated by commas. Or, enter a range of ports separated by a dash.

At the bottom of the page, it says 'Copyright © 2011 Allied Telesis Inc. All rights reserved.' and 'www.alliedtelesis.com'.

Figure 42. Multicast MAC Address Page

4. Add a new multicast MAC address, do the following:

- MAC Address**— Enter a multicast MAC address. Use the following format:

XX:XX:XX:XX:XX:XX

- Port Number**— Select the port number which the end node of the MAC address is connected.

- VLAN**— Select a VLAN where the port is a member.
- Action**— Select one of the following options:
 - Forward:** Specifies the port to forward packets that have the designated source MAC address.
 - Discard:** Specifies the port to discard packets that have the designated source MAC address.

5. Click **Add**.
6. Click **SAVE** to save your changes to the startup configuration file.

Deleting a Unicast MAC Address

To delete a unicast address or clear all static or dynamic unicast addresses, do the following:

1. Select the Switching tab.

The Switching tab is displayed. See Figure 38 on page 108.

2. Select **MAC Table** and then move the cursor to the right to select **Unicast**.

The Unicast MACs page is displayed. See Figure 39 on page 108.

3. Do one of the following:

- To clear all of the static unicast addresses in the MAC address table, click [Clear Static](#).
- To clear the dynamic unicast addresses in the MAC address table, click [Clear Dynamic](#).
- To delete a specific MAC address, click [Delete](#) next to the MAC address that you want to delete.

Deleting a Multicast MAC Address

To delete a multicast address or clear all static or dynamic multicast addresses, do the following:

1. Select the Switching Tab.

The Switching Tab is displayed. See Figure 38 on page 108.

2. Select **Mac Table** and then move the cursor to the right to select **Multicast**.

The Multicast MACs page is displayed. See Figure 40 on page 110.

3. Do one of the following:

- To clear all of the static multicast addresses in the MAC address table, click Clear Static.
- To clear all of the dynamic multicast addresses in the MAC address table, click Clear Dynamic.
- To delete a specific MAC address, click Delete next to the MAC address that you want to delete.

Chapter 9

Link Aggregation Control Protocol (LACP)

LACP is used to increase the bandwidth between the switch and other LACP-compatible devices by grouping ports together to form single virtual links.

This chapter provides a brief description of LACP and explains how to display and set LACP. See the following sections:

- “Overview” on page 118
- “Displaying LACP Trunks” on page 119
- “Adding an LACP Trunk” on page 121
- “Modifying an LACP Trunk” on page 123
- “Deleting an LACP Trunk” on page 125

For more information about LACP trunks, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Link Aggregation Control Protocol (LACP)
- LACP Commands

Overview

LACP trunks are similar in function to static port trunks, but they are more flexible. The implementations of static trunks tend to be vendor specific and may not always be compatible. In contrast, the implementation of LACP in the switch is compliant with the IEEE 802.3ad standard. It is interoperable with equipment from other vendors that also comply with the standard. This makes it possible to create LACP trunks between the switch and network devices from other manufacturers.

The main component of an LACP trunk is an aggregator. An aggregator is a group of ports on the switch. The ports of an aggregator are further grouped into a trunk, referred to as an aggregate trunk. An aggregator can have only one trunk. You have to create a separate aggregator for each trunk on the switch.

An aggregate trunk can consist of any number of ports on the switch, but only a maximum of eight ports can be active at a time. If an aggregate trunk contains more ports than can be active at one time, the extra ports are placed in standby mode. Ports in standby mode do not pass network traffic, but they do transmit and accept LACP data unit (LACPDU) packets, which the switch uses to search for LACP-compliant devices.

Displaying LACP Trunks

To display the LACP trunk assignments for all of the switch ports, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 43.

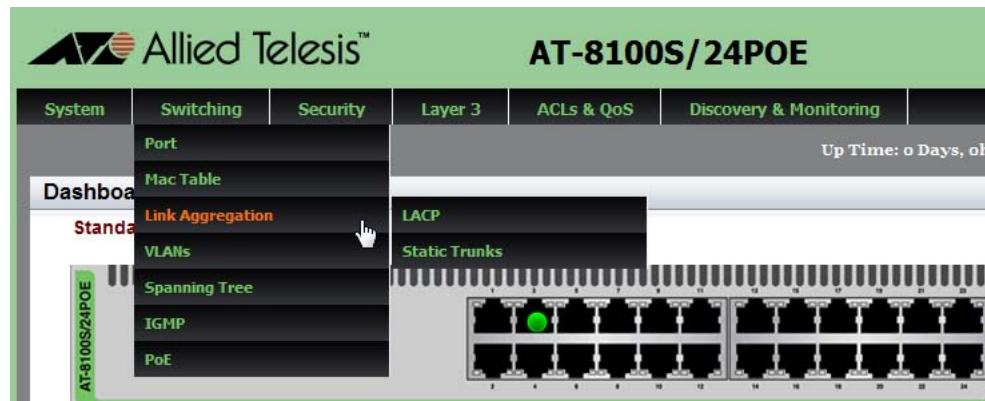


Figure 43. Switching Tab with Link Aggregation Selected

3. Move the cursor to the right and select **LACP**.

The LACP Trunks page is displayed. See Figure 44.

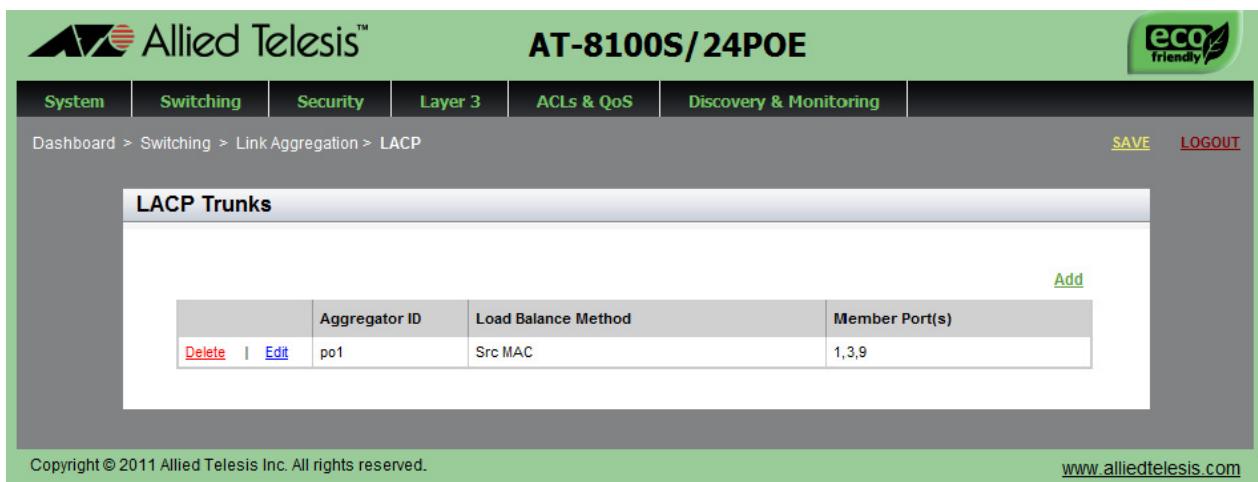


Figure 44. LACP Trunks Page

4. The following fields are displayed:

- Aggregator ID**— The Aggregator ID number is the base port number (or lowest port number) of an aggregator. For instance, an aggregator of ports 12, 16 and 17 is assigned the ID number 12.
- Load Balance Method**— Indicates the load distribution methods of the aggregators. An aggregator can have only one load distribution method. The load distribution method determines the manner in which the switch distributes the egress packets among the active ports of an aggregator. The packets can be distributed by source MAC or IP address, destination MAC or IP address, or by both source and destination addresses.
- Member Port(s)**— Displays the member ports of the aggregator.

Adding an LACP Trunk

To create an LACP trunk, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 43 on page 119.

3. Move the cursor to the right and select **LACP**.

The LACP Trunks page is displayed. See Figure 44 on page 119.

4. From the LACP Trunks page, click Add.

The Add LACP Trunk page is displayed. See Figure 45.

The screenshot shows the 'Add LACP Trunk' configuration page. At the top, the navigation bar includes tabs for System, Switching (which is selected), Security, Layer 3, ACLs & QoS, and Discovery & Monitoring. The page title is 'AT-8100S/24POE'. The main content area is titled 'Add LACP Trunk'. It contains the following fields:

- Aggregator ID**: A text input field with '(1-32)' placeholder text.
- Load Balance Method**: A dropdown menu set to 'Src-Dst MAC'. Below it, a 'Default' label is followed by 'Src-Dst Mac'.
- Member Port**: A grid of 26 checkboxes arranged in two rows of 13. The first row contains checkboxes for ports 1, 3, 5, 7, 9, 11, 13, 15, 17, 19, 21, 23, and 25. The second row contains checkboxes for ports 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, and 26.

On the right side of the page, a 'HELP' box provides the following information:

- Aggregator ID**: Describes it as an ID number for an aggregator port, noting it must be the base port number of an aggregator (e.g., ports 15, 16, and 17 assigned ID 15).
- Load Balance Method**: Describes it as a selection from a dropdown menu, with 'Src MAC' as an option.
- Src MAC**: A bullet point listing 'Src MAC' as a specification for source MAC address as the load distribution method.

At the bottom of the page, there is an 'Add' button and a copyright notice: 'Copyright © 2011 Allied Telesis Inc. All rights reserved.' and the website 'www.alliedtelesis.com'.

Figure 45. Add LACP Trunk Page

5. Enter an aggregator ID number in the **Aggregator ID** field. The number must be the base port number (or lowest port number) of an aggregator. For instance, an aggregator of ports 12,16 and 17 is assigned the ID number 12.
6. Select the Load Balance Method. Choose from the following:
 - Src MAC**— Specifies source MAC address as the load distribution method.
 - Dst MAC**— Specifies destination MAC address as the load distribution method.
 - Src-Dst MAC**— Specifies source address and destination MAC address as the load distribution method.
 - Src IP**— Specifies source IP address as the load distribution method.
 - Dst IP**— Specifies destination IP address as the load distribution method.
 - Src-Dst IP**— Specifies source address and destination IP address as the load distribution method.
7. Click a port number to add to the aggregator. A green check mark indicates a port has been selected. You can select multiple ports.
To deselect a port, click the box that indicates the port number.
8. Click **Add**.
A confirmation message is displayed.
9. Click **SAVE** to save your changes to the startup configuration file.

Modifying an LACP Trunk

To modify the LACP Trunk settings, see the following procedure:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 43 on page 119.

3. Move the cursor to the right and select **LACP**.

The LACP Trunks page is displayed. See Figure 44 on page 119.

4. From the LACP Trunks page, click Edit next to the Aggregator ID that you want to change.

The Modify LACP Trunk page is displayed. See Figure 46.

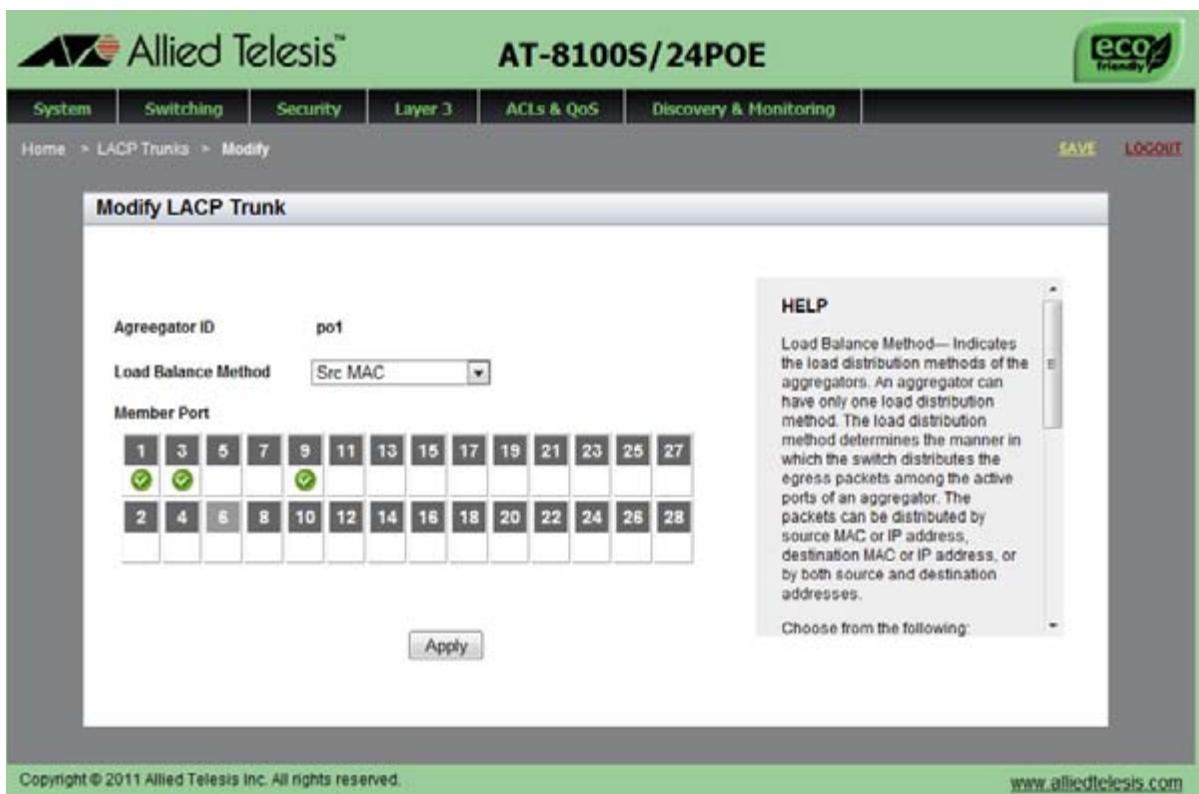


Figure 46. Modify LACP Trunk Page

5. Select the Load Balance Method. Choose from the following:
 - Src MAC**— Specifies source MAC address as the load distribution method.
 - Dst MAC**— Specifies destination MAC address.
 - Src-Dst MAC**— Specifies source address/destination MAC address.
 - Src IP**— Specifies source IP address.
 - Dst IP**— Specifies destination IP address.
 - Src-Dst IP**— Specifies source address/destination IP address.
6. Add or remove the member ports of the aggregator by clicking on the ports.

A check mark indicates the port has been selected.

Note

You cannot add ports that have lower port number than the base port number (lowest port number) of an aggregator. Also, you are not allowed to remove the port with the lowest port number of an aggregator. Because the aggregator ID number is the base port number of an aggregator, adding or removing the port with the lowest port number causes a conflict with the aggregator ID number.

7. Click **Apply**.

A confirmation message is displayed.

8. Click **SAVE** to save your changes to the startup configuration file.

Deleting an LACP Trunk

To delete an LACP trunk, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 43 on page 119.

3. Move the cursor to the right and select **LACP**.

The LACP Trunks page is displayed. See Figure 44 on page 119.

4. From the LACP Trunks page, click Delete next to the Aggregator ID that you want to delete.

5. Click **SAVE** to save your changes to the startup configuration file.

Chapter 10

Setting Static Port Trunks

Static port trunks are groups of two to eight ports that act as single virtual links between the switch and other network devices. This chapter describes how to display, create, and modify static trunks. See the following sections:

- “Overview” on page 128
- “Displaying Static Trunk Settings” on page 129
- “Adding Static Trunks” on page 131
- “Modifying the Static Trunk Settings” on page 134
- “Deleting Static Trunks” on page 137

For additional guidelines and information regarding static port trunks, see following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Static Port Trunks
- Static Port Trunk Commands

Overview

Static port trunks are commonly used to improve network performance by increasing the available bandwidth between the switch and other network devices as well as to enhance the reliability of the connections between network devices.

When you create a static port trunk, you can designate how the traffic is distributed across the physical links of the switch by defining the load distribution method.

Static port trunks do not permit standby ports, unlike LACP trunks (which are described in Chapter 9, “Link Aggregation Control Protocol (LACP)” on page 117). If a link is lost on a port in a static port trunk, the trunk’s total bandwidth is reduced. Although the traffic carried by a lost link is shifted to one of the remaining ports in the trunk, the bandwidth remains reduced until a lost link is reestablished or another port is manually added to the trunk.

Here are some guidelines regarding static port trunks:

- A static trunk can have up to eight ports.
- The switch supports up to a total of 32 static port trunks and LACP trunks at a time. An LACP trunk is counted against the maximum number of trunks when it is active.
- The ports of a static port trunk can be all twisted pair ports or all fiber optic ports. Static port trunks *cannot* have both types of ports.
- The ports of a trunk can be consecutive (for example ports 5-9) or nonconsecutive (for example, ports 4, 8, 11, 20).

Displaying Static Trunk Settings

To display the static port trunks for all of the switch ports, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Link Aggregation**.

For an example of the Link Aggregation tab, see Figure 47.



Figure 47. Switching Tab with Static Trunks

3. Move the cursor to the right and select **Static Trunks**.

The Static Trunks page is displayed as shown in Figure 48. By default, no static trunks are specified on the switch.

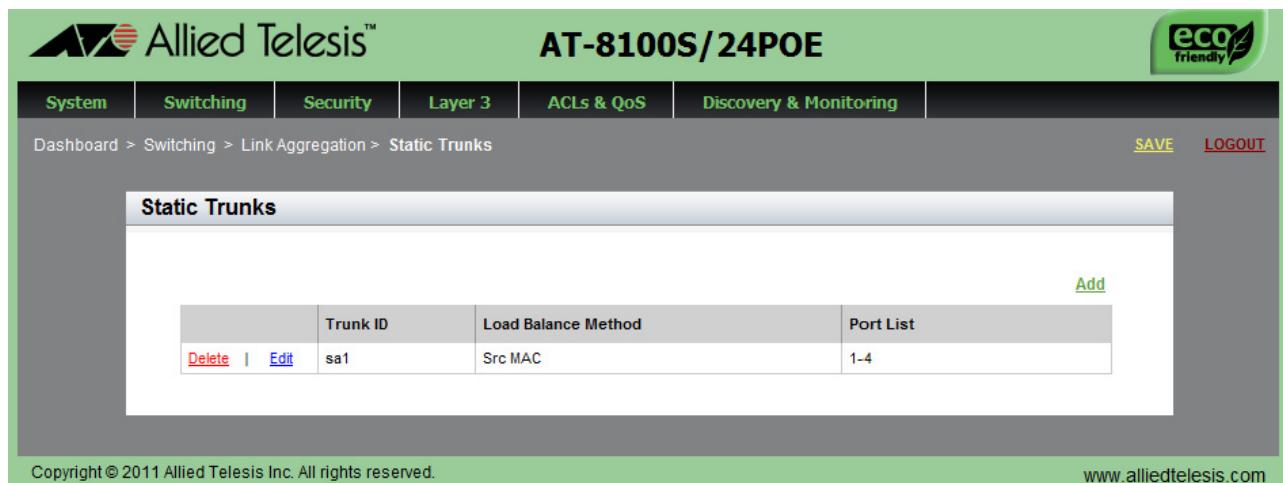


Figure 48. Static Trunks Page

The following fields are displayed:

- Trunk ID**— Indicates the ID number of the static trunk.
- Load Balance Method**— Indicates one of the following:
 - Src MAC**: Specifies source MAC address as the load distribution method.
 - Dst MAC**: Specifies destination MAC address as the load distribution method.
 - Src -Dst MAC**: Specifies source address and destination MAC address as the load distribution method.
 - Src IP**: Specifies source IP address as the load distribution method.
 - Dst IP**: Specifies destination IP address as the load distribution method.
 - Src-Dst IP**: Specifies source address and destination IP address as the load distribution method.
- Port List**— Displays the list of ports that are members of the static trunk.

Adding Static Trunks

Review the following information before creating a new static port trunk:

- When you create a new trunk, the settings of the lowest numbered port are copied to the other ports so that all the ports have the same settings. Therefore, you must examine and verify that the speed, duplex mode, and flow control settings of the lowest numbered port are correct for the network device to which the trunk is connected.
- All ports of a trunk must be members of the same VLAN.
- Ports can be members of one static port trunk at a time. A port that is already a member of a trunk cannot be added to another trunk. To accomplish this, you must remove the member port from its current trunk assignment first. For instructions, see "Adding Static Trunks" on page 131.

To create an static port trunk, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 47 on page 129.

3. Move the cursor to the right and select **Static Trunks**.

The Static Trunks page is displayed. See Figure 48 on page 129.

4. From the Static Trunks page, click Add.

The Add Static Trunk page is displayed. See Figure 49 on page 132.

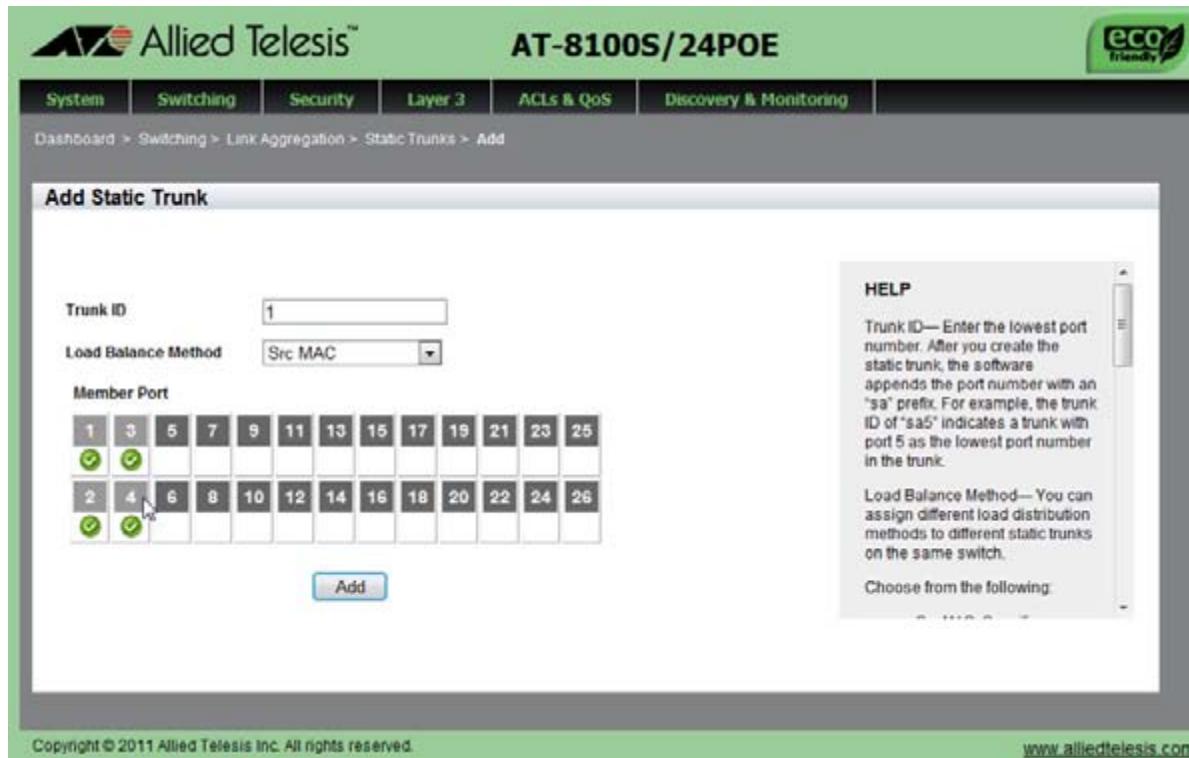


Figure 49. Add Static Trunk Page

5. Assign an ID number of a new static trunk in the **Trunk ID** field. The range is 1 to 32.
6. Select the **Load Balance Method**. You can assign different load distribution methods to different static trunks on the same switch.

Choose from the following:

- Src MAC**— Specifies source MAC address as the load distribution method.
- Dst MAC**— Specifies destination MAC address as the load distribution method.
- Src-Dst MAC**— Specifies source address and destination MAC address as the load distribution method.
- Src IP**— Specifies source IP address as the load distribution method.
- Dst IP**— Specifies destination IP address as the load distribution method.
- Src-Dst IP**— Specifies source address and destination IP address as the load distribution method.

7. Select a member port in the **Member Port** table by clicking a box that indicates a port number. You can select multiple ports. A green check mark indicates a port has been selected.

To deselect a port, click the box that indicates the port number.

8. Click **Add**.

A confirmation message is displayed.

9. Click **SAVE** to save your changes to the startup configuration file.

Modifying the Static Trunk Settings

Review the following information if you are adding ports to an existing trunk:

- The ports of a static trunk must be members of the same VLAN.
- If the new port added to a trunk is already a member of another static trunk, you must first remove it from its current trunk assignment.

To add or remove member ports from a static port trunk, or modify the load balance method, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 47 on page 129.

3. Move the cursor to the right and select **Static Trunks**.

The Static Trunks page is displayed. See Figure 48 on page 129.

4. From the Static Trunks page, click Edit.

The Modify Static Trunk page is displayed. See Figure 50 on page 135.

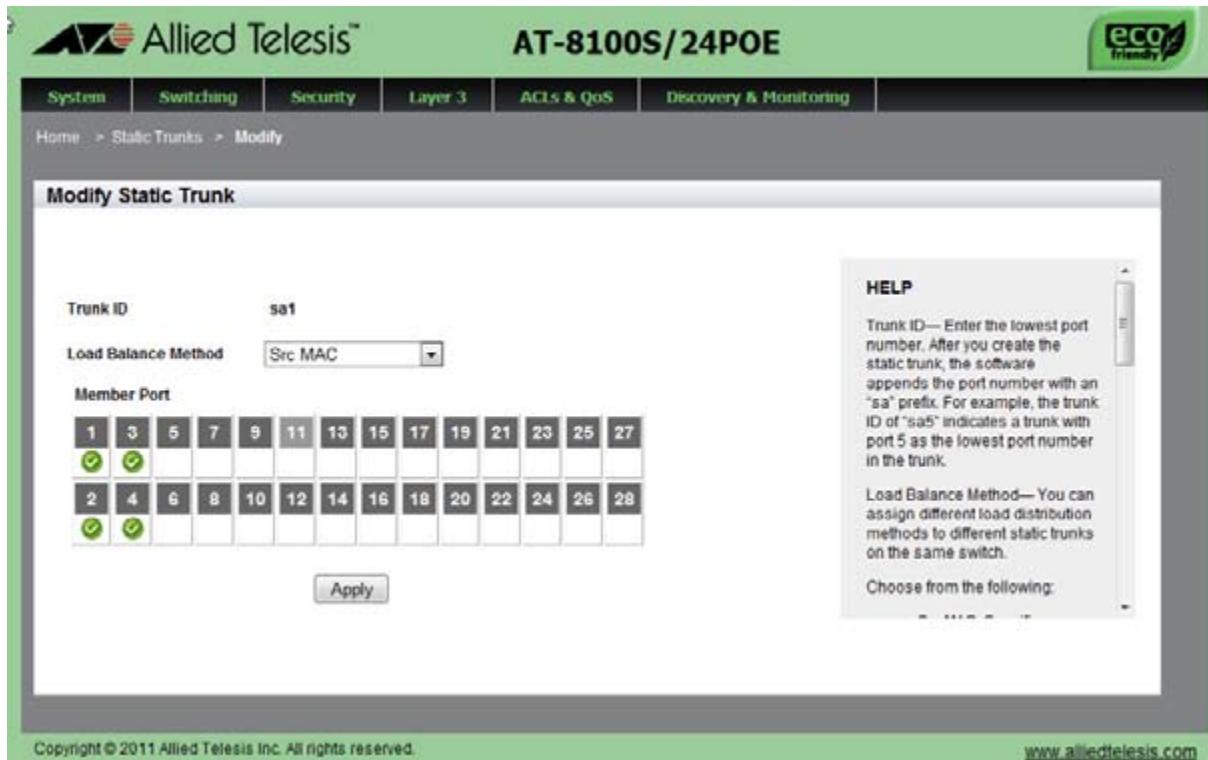


Figure 50. Modify Static Trunk Page

5. Change the **Load Balance Method** as needed. You can assign different load distribution methods to different static trunks on the same switch.

Choose from the following:

- Src MAC**— Specifies source MAC address as the load distribution method.
- Dst MAC**— Specifies destination MAC address as the load distribution method.
- Src-Dst MAC**— Specifies source address/destination MAC address as the load distribution method.
- Src IP**— Specifies source IP address as the load distribution method.
- Dst IP**— Specifies destination IP address as the load distribution method.
- Src-Dst IP**— Specifies source address/destination IP address as the load distribution method.

6. Select the member ports that you want to add to or remove from the static trunk by clicking on the ports.



Caution

To prevent the formation of network loops in your network topology, do not remove ports from a static port trunk without first disconnecting their network cable. Network loops can result in broadcast storms that can adversely affect network performance.

Note

You cannot have a trunk that contains only one port. There must be a minimum of two ports in a trunk.

7. Click **Apply**.

A confirmation message is displayed.

8. Click **SAVE** to save your changes to the startup configuration file.

Deleting Static Trunks

To delete a static port trunk, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Link Aggregation**.

For an example of the Link Aggregation selection, see Figure 47 on page 129.

3. Move the cursor to the right and select **Static Trunks**.

The Static Trunks page is displayed. See Figure 48 on page 129.

4. From the Static Trunks page, click Delete next to the Trunk ID that you want to delete.

Chapter 11

Setting Port-based and Tagged VLANs

This chapter provides a brief description of VLANs and explains how to display, create, and modify port-based and tagged VLANs. See the following sections:

- “Overview” on page 140
- “Displaying VLANs” on page 142
- “Adding an VLAN” on page 143
- “Modifying VLANs” on page 145
- “Assigning a Native VLAN” on page 148
- “Removing an Untagged Port from a VLAN” on page 150
- “Deleting VLANs” on page 152

For additional information about VLANs, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Port-based and Tagged VLANs
- Port-based and Tagged VLAN Commands

Overview

A VLAN is a group of ports that form a logical Ethernet segment on an Ethernet switch. The ports of a VLAN form an independent broadcast domain in which the traffic generated by the nodes remains within the VLAN.

VLANs let you segment your network through the switch's management software so that you can group nodes with related functions into their own separate, logical LAN segments. These VLAN groupings can be based on similar data needs or security requirements. For example, you can create separate VLANs for the different departments in your company, such as one for Sales and another for Accounting. Setting port-based and tagged VLANs is supported in the web interface.

Port-based VLANs

A port-based VLAN is a group of ports on an Ethernet switch that form a logical Ethernet segment. Each port of a port-based VLAN can belong to only one VLAN at a time. A port-based VLAN can have as many or as few ports as needed. The VLAN can consist of all the ports on an Ethernet switch, or just a few ports. In addition, a port-based VLAN can span switches and consist of ports from multiple Ethernet switches.

Ports in a port-based VLAN are referred to as *untagged ports* and the frames received on the ports as *untagged frames*. The names derive from the fact that the frames received on a port do not contain any information that indicates VLAN membership, and that VLAN membership is determined solely by a port's PVID.

Port VLAN Identifier

Each port in a port-based VLAN must have a port VLAN identifier (PVID). The switch associates a frame to a port-based VLAN by the PVID assigned to a port on which a frame is received, and forwards a frame only to those ports with the same PVID. Consequently, all ports of a port-based VLAN must have the same PVID. In addition, the PVID of the ports in a VLAN must match the VLAN's VID.

For example, if you create a port-based VLAN on the switch and assign it the VID 5, the PVID for each port in the VLAN needs to be assigned the value of 5.

Tagged VLANs

The second type of VLAN is the tagged VLAN. VLAN membership in a tagged VLAN is determined by information within the frames that are received on a port. This differs from a port-based VLAN, where the PVIDs assigned to the ports determine VLAN membership.

The VLAN information within an Ethernet frame is referred to as a *tag* or *tagged header*. A tag, which follows the source and destination addresses in a frame, contains the VID of the VLAN to which the frame belongs (IEEE 802.3ac standard). This number uniquely identifies each VLAN in a network.

When the switch receives a frame with a VLAN tag, referred to as a *tagged frame*, the switch forwards the frame only to those ports that share the same VID.

A port that receives or transmits tagged frames is referred to as a *tagged port*. Any network device connected to a tagged port must be IEEE 802.1Q-compliant. This is the standard that outlines the requirements and standards for tagging. The device must be able to process the tagged information on received frames and add tagged information to transmitted frames.

Tagged and Untagged Ports

You need to specify which ports are members of the VLAN. In the case of a tagged VLAN, it is usually a combination of both untagged ports and tagged ports. You specify which ports are tagged and which untagged when you create the VLAN.

An untagged port, whether a member of a port-based VLAN or a tagged VLAN, can be in only one VLAN at a time. However, a tagged port can be a member of more than one VLAN. A port can also be an untagged member of one VLAN and a tagged member of different VLANs simultaneously.

Native VLAN

A tagged port supports traffic coming from multiple VLANs (tagged traffic) as well as traffic that does not come from a VLAN (untagged traffic). If a native VLAN is assigned to the tagged port, when the tagged port receives untagged frames, it forwards those frames to the native VLAN.

Displaying VLANs

To display the VLAN assignments for all of the switch ports, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **VLANs**.

The VLANs page is displayed. For an example of the VLANs page, see Figure 51.

	Vlan ID	Name	Untagged Member Ports	Tagged Member Ports
Edit	1	Default_VLAN	2-10	
Delete Edit	2	techpub	11-24	1
Delete Edit	3	engineering	25-26	1
Delete Edit	99	management		

Figure 51. VLANs Page

The following fields are displayed:

- **Vlan ID**— Indicates a VLAN identifier. The range is 1 to 4094. The VID of 1 is the default VLAN.
- **Name**— Indicates a name of a VLAN.
- **Untagged Member Ports**— Indicates untagged ports that belong to the VLAN.
- **Tagged Member Ports**— Indicates tagged ports that belong to the VLAN.

Note

By default, there is one VLAN configured. This is the default VLAN with a Vlan ID of 1. All ports on the switch are assigned to the default VLAN. All ports in Vlan ID 1 are untagged by default.

Adding an VLAN

To create an VLAN, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **VLANs**.

The VLANs page is displayed. See Figure 51 on page 142.

3. From the VLANs page, click Add.

The Add VLAN page is displayed. See Figure 52.

The screenshot shows the 'Add VLAN' page of the AT-8100S/24POE web interface. The top navigation bar includes tabs for System, Switching, Security, Layer 3, ACLs & QoS, and Discovery & Monitoring. The 'Switching' tab is selected. Below the tabs, the breadcrumb navigation shows 'Dashboard > Switching > VLANs > Add'. On the right, there are 'SAVE' and 'LOGOUT' buttons. The main content area is titled 'Add VLAN'. It contains fields for 'VLAN Id' and 'VLAN Name', both of which are currently empty. To the right of these fields is a 'HELP' box with the following text:

HELP

VLAN ID—Specifies a VLAN identifier. The range is 2 to 4094. The VID 1 is reserved for the Default_VLAN. The VID cannot be the same as the VID of an existing VLAN on the switch. If this VLAN is unique in your network, its VID must also be unique. However, if this VLAN is part of a larger VLAN

Below the fields are two rows of 25 numbered boxes, representing port numbers 1 through 25. The second row contains boxes for ports 2, 4, 6, 8, 10, 12, 14, 16, 18, 20, 22, 24, and 26. To the right of these boxes are four buttons: 'All Tagged', 'All Untagged', 'Deselect All', and 'Native Vlans'. At the bottom of the page are 'Add' and 'Cancel' buttons. The footer of the page includes the copyright notice 'Copyright © 2011 Allied Telesis Inc. All rights reserved.' and the website 'www.alliedtelesis.com'.

Figure 52. Add VLAN Page

4. Enter the following settings as needed:

- VLAN ID**— Assign a VLAN identifier. The range is 2 to 4094. The VID 1 is reserved for the Default_VLAN. The VID cannot be the same as the VID of an existing VLAN on the switch.

If this VLAN is unique in your network, its VID must also be unique. However, if this VLAN is part of a larger VLAN that spans multiple switches, the VID value for the VLAN must be the same on each switch. For example, if you are creating a VLAN called Sales with a VID of 3 that spans three switches, assign the Sales VLAN on each switch the VID value of 3.

- VLAN Name**— Specify the name of a VLAN. The name can be from 1 to 20 characters in length. The first character must be a letter; it cannot be a number. The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). You cannot assign the name of name of an existing VLAN on the switch.

VLANs are easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). If a VLAN is unique in your network, then its name must be unique as well. A VLAN that spans multiple switches must have the same name on each switch.

- Member Port**— Click a port number to add the port to the VLAN. A “T” indicates a port is a tagged port. A “U” indicates the port is an untagged port.

Note

For information about tagged and untagged ports, see “Overview” on page 140.

- All Tagged**— Click this button to make all ports on the switch tagged ports.
- All Untagged**— Click this button to make all ports on the switch untagged ports.
- Deselect All**— Click this button to deselect, or unclick, all of the selected ports.

5. Click **Apply**.

A confirmation message is displayed.

6. Click **SAVE** to save your changes to the startup configuration file.

Modifying VLANs

To modify the LACP Trunk settings, see the following procedure:



Caution

Modifying the VLAN membership of active ports may cause loss of connectivity to the switch.

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **VLANs**.

The VLANs page is displayed. See Figure 51 on page 142.

3. From the VLANs page, click Edit next to the VLAN ID that you want to modify.

The Modify VLAN page is displayed. See Figure 53 on page 146.

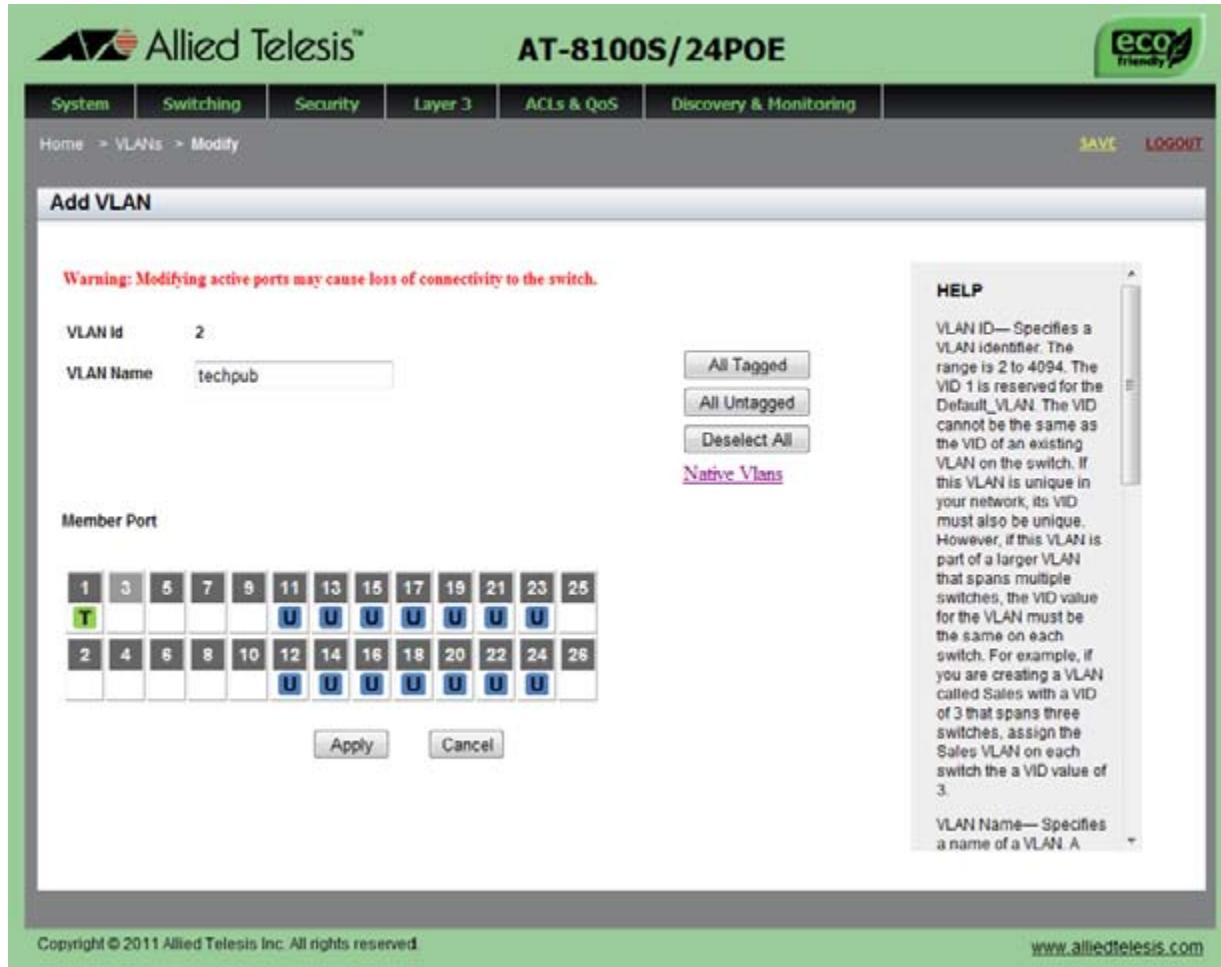


Figure 53. Modify VLAN Page

4. Change the following fields as needed:

- VLAN Name**—Change the name of a VLAN. The name can be from 1 to 20 characters in length. The first character must be a letter; it cannot be a number. A name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!). You cannot assign the name of an existing VLAN on the switch.

VLANs are easier to identify if their names reflect the functions of their subnetworks or workgroups (for example, Sales or Accounting). If a VLAN is unique in your network, then its name must be unique as well. A VLAN that spans multiple switches must have the same name on each switch.

- Member Port**—Assign either “T” or “U” by clicking a port number. A “T” indicates the port is a tagged port. A “U” indicates the port is an untagged port. To remove the port from the VLAN, uncheck the port.

Note

When a port does not have any mark, the port belongs to the default VLAN. When you assign an “H” to a port, the switch removes the untagged port from the VLAN and also removes the untagged port from the default VLAN. For more information, see “Removing an Untagged Port from a VLAN” on page 150.

- All Tagged**— Click this button to make all ports on the switch tagged ports.
- All Untagged**— Click this button to make all ports on the switch untagged ports.
- Deselect All**— Click this button to deselect, or unclick, all of the selected ports.

5. Click **Apply**.

A confirmation message is displayed.

6. Click **SAVE** to save your changes to the startup configuration file.

Assigning a Native VLAN

A VLAN can be assigned to a tagged port so that untagged ingress traffic is placed on the VLAN. This VLAN is referred to as the native VLAN.

To assign a native VLAN to a tagged port, perform the following procedure:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **VLANs**.

The VLANs page is displayed. See Figure 51 on page 142.

3. From the VLANs page, click Add.

The Add VLAN page is displayed. See Figure 52 on page 143.

4. From Add VLANs page, click Native VLAN.

The Native VLAN page is displayed. See Figure 54.

Native Vlan

VLAN Interface: 1

Port ID: port1.0.1

HELP

This option changes a Tagged port's Native VLAN. Choose the Port ID and specify its Native VLAN. The native VLAN is used for classifying the incoming untagged packets. Default: VLAN ID 1.

Figure 54. Native VLAN Page

5. Change the following fields as needed:

- VLAN Interface**— Select a VLAN ID from the pull-down menu. The selected VLAN Interface is assigned to a port as a native VLAN, which untagged frames are placed on.
- Port ID**— Select a port ID from the pull-down menu. You can only select a tagged port.

6. Click **Create**.

A confirmation message is displayed.

7. Click **SAVE** to save your changes to the startup configuration file.

Removing an Untagged Port from a VLAN

By default, all the ports on the switch belong to the default-VLAN, VLAN1 as untagged ports. When you assign a port to another VLAN as an untagged port, the switch removes the untagged port from the original VLAN, and then assigns it to the new VLAN.



Caution

Modifying the VLAN membership of active ports may cause loss of connectivity to the switch.

To remove a untagged port from the VLAN and leave the port not belong to any VLAN, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **VLANs**.

For an example of the VLANs page is displayed, see Figure 51 on page 142.

3. From the VLANs page, click Edit next to the VLAN that the untagged port you want to remove is belong to.

The Modify VLAN page is displayed. See Figure 55 on page 151.

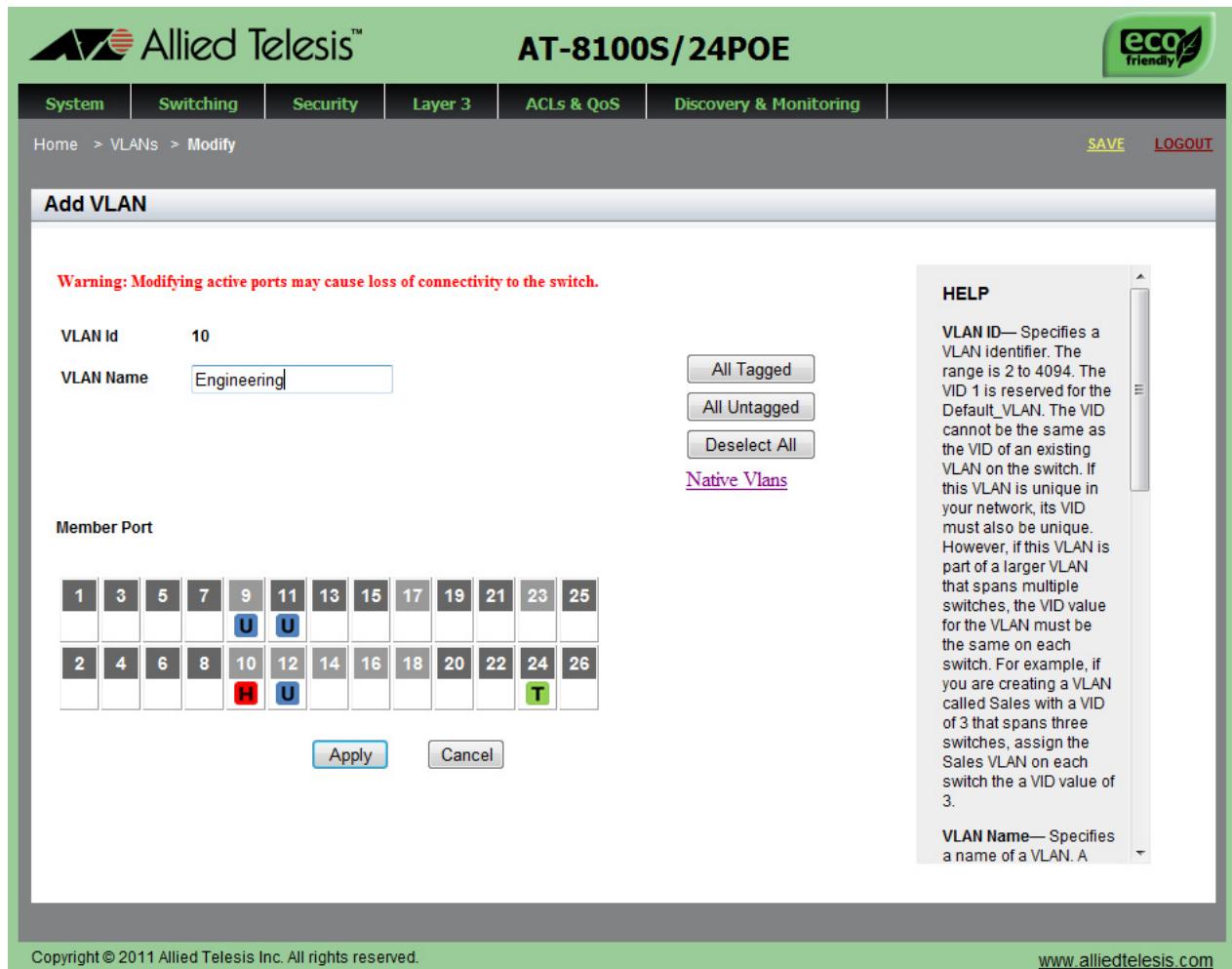


Figure 55. Modify VLAN Page

4. Click a port number a couple of times to check the port with an “H” mark. An “H” indicates the port is removed from all VLANs on the switch as an untagged port.

Note

When you remove a “U” mark from a port and leave no mark on the port, and then click **Apply**, the switch removes the port from the VLAN and assigns it to the default-VLAN as an untagged port. When you check a port with an “H” mark, the switch removes the port from the VLAN, but does not assign it to any VLAN. Even when a port does not belong to any VLAN as an untagged port, the port can be a member of a VLAN as a tagged port.

5. Click **Apply**.

Deleting VLANs



Caution

Deleting VLANs that active ports belong to may cause loss of connectivity to the switch.

To delete an VLAN, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **VLANs**.

For an example of the Virtual LANs page is displayed, see Figure 51 on page 142.

3. From the VLANs page, click Delete next to the VLAN that you want to remove.

The selected VLAN is removed.

Note

You cannot remove the default VLAN which has an Vlan ID of 1.

Chapter 12

Spanning Tree Protocols on the Switch

This chapter provides a brief description of both the Spanning Tree Protocol (STP) and the Rapid Spanning Tree Protocol (RSTP) and explains how to set the spanning tree protocols on the switch. See the following sections:

- “Overview” on page 154
- “Displaying and Modifying Spanning Tree Protocol Settings on the Switch” on page 155

Note

For information about how to set a spanning tree protocol on the ports, see Chapter 7, “Spanning Tree Protocol on a Port” on page 99.

For more information about spanning tree, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Spanning Tree and Rapid Spanning Tree Protocols
- Spanning Tree Protocol (STP)
- STP Commands
- Rapid Spanning Tree Protocol (RSTP)
- RSTP Commands

Overview

Both STP and RSTP guard against the formation of loops in an Ethernet network topology. A topology has a loop when two or more nodes can transmit packets to each other over more than one data path. Packets can become caught in repeating cycles, referred to as broadcast storms, that needlessly consume network bandwidth and that can significantly reduce network performance.

STP and RSTP prevent loops from forming by ensuring that only one path exists between the end nodes in your network. Where multiple paths exist, these protocols place the extra paths in a standby or blocking mode. In addition, STP and RSTP can activate redundant paths if primary paths go down. These protocols guard against multiple links between segments and the risk of broadcast storms and maintain network connectivity by activating backup redundant paths.

One of the primary differences between the two protocols is in the time each takes to complete the process referred to as convergence. When a change is made to the network topology, such as the addition of a new bridge, a spanning tree protocol determines whether there are redundant paths that must be blocked to prevent data loops, or activated to maintain communications between the various network segments. This is the process of convergence.

With STP, convergence can take up to a minute to complete in a large network. This can result in the loss of communication between various parts of the network during the convergence process, and the subsequent lost of data packets.

RSTP is much faster than STP. It can complete a convergence in seconds, and so greatly diminish the possible impact the process can have on your network. Only one spanning tree can be active on the switch at a time. The default setting is RSTP.

The AT-8100 Series switch supports MSTP; however, the Web Browser Interface does not support MSTP configuration. You must use the CLI to configure MSTP on the switch. See “Multiple Spanning Tree Protocol” in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*.

Displaying and Modifying Spanning Tree Protocol Settings on the Switch

To display and modify Spanning Tree Protocol settings on the switch, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 24 on page 69.

2. From the Switching tab, select **Spanning Tree**.

The Spanning Tree Settings page is displayed. See Figure 56.

The screenshot shows the 'Spanning Tree Settings' page of the Allied Telesis AT-8100S/24POE web interface. The page has the following fields:

- Active Protocol:** RSTP (selected from a dropdown menu)
- Status:** Enabled (selected from a dropdown menu)
- Bridge Priority:** 32768 (input field)
- Hello Time:** 2 (input field)
- Forward Delay:** 15 (input field)
- Max Age:** 20 (input field)
- BPDU Guard:** Disabled (selected from a dropdown menu)

Below the input fields is an 'Apply' button. To the right of the input fields is a 'HELP' panel with the following text:

HELP

Active Protocol—Select the spanning tree protocol from the pull-down menu. The options are STP, RSTP, and MSTP. The default setting is RSTP.

Status—Select Enabled or Disabled from the pull-down menu. By default, the spanning tree protocol is enabled.

Current Priority—Indicates the current value of the. By default, the current priority is set to 32,768. You cannot change this field.

New Priority (0-15)—Assign the switch a bridge priority number using an increment. The range is 0 to 15.

At the bottom of the page, there is a copyright notice: Copyright © 2011 Allied Telesis Inc. All rights reserved. and a website link: www.alliedtelesis.com.

Figure 56. Spanning Tree Settings Page

The following fields are displayed. Change the settings as needed:

- Active Protocol**— Select the spanning tree protocol from the pull-down menu. The options are STP and RSTP. The default setting is RSTP.
- Status**— Enable or disable the spanning tree protocol on the switch. By default, the spanning tree protocol is enabled.
- Bridge Priority**— Assign the switch a bridge priority number. The device that has the lowest priority number in the spanning tree domain becomes the root bridge. You can use the priority number to influence which switch becomes the root bridge. If two or more devices have the same priority value, the device with the numerically lowest MAC address becomes the root bridge.

The actual range is 0 to 61440 in increments of 4096, for a total of 16 increments, shown in Table 2. You specify the increment of the value, from 0 to 15. The default is 32768, which is increment 8.

Table 2. STP Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Note

Set the hello time, forward delay, and max-age fields according to the following formulas, as specified in IEEE Standard 802.1d:

max-age $\leq 2 \times (\text{forward time} - 1.0 \text{ second})$
 max-age $\geq 2 \times (\text{hello time} + 1.0 \text{ second})$

- Hello Time**— Enter the hello time in seconds. The hello time is the frequency that the switch sends bridge protocol data units (BPDUs), which contain spanning tree configuration information. The range is 1 to 10 seconds.

This value is active only when the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

- Forward Delay**— Enter the forward delay time in seconds. The forward delay specifies how long the ports remain in the listening and learning or discarding states before they transition to the forwarding state. The range is 4 to 30 seconds.

This value is active only when the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

- Max Age**— Enter the max age in seconds. The max age determines how long BPDUs are stored by the switch before they are deleted. The default setting is 20 seconds. The range is 6 to 40 seconds.

This value is active only when the switch is acting as the root bridge of the spanning tree domain. Switches that are not acting as the root bridge use a dynamic value supplied by the root bridge.

- BPDU Guard**— Enable or disable the BPDU guard feature on the switch. When the BPDU guard feature is enabled on the switch, the switch monitors edge ports and disables them if they receive BPDU packets.

3. Click **Apply**.
4. Click **SAVE** to save your changes to the startup configuration file.

Chapter 13

Internet Group Management Protocol (IGMP) Snooping

This chapter provides a brief description of IGMP Snooping and explains how to set this feature on the switch. See the following sections:

- “Overview” on page 160
- “Displaying and Modifying IGMP Snooping Configuration” on page 161
- “Disabling IGMP Snooping” on page 164
- “Displaying the Routers List” on page 165
- “Clearing the Routers List” on page 167
- “Displaying the Hosts List” on page 168

For more information about IGMP, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Internet Group Management Protocol (IGMP) Snooping
- IGMP Commands

Overview

IGMP snooping allows the switch to control the flow of multicast packets from its ports. It enables the switch to forward packets of a multicast group to only ports connected to members of the multicast group. When the switch is not using IGMP snooping and receives multicast packets, it floods the packets out all its ports, except the port on which it received the packets. Such flooding of packets can negatively impact network performance.

IGMP is used by IPv4 routers to create lists of nodes that are members of multicast groups. A multicast group is a group of end nodes that want to receive multicast packets from a multicast application. The router creates a multicast membership list by periodically sending out queries to the local area networks connected to its ports.

A node that wants to become a member of a multicast group responds to a query by sending a report. A report indicates that an end node wants to become a member of a multicast group. Nodes that join a multicast group are referred to as host nodes. After joining a multicast group, a host node must continue to periodically issue reports to remain a member.

After the router has received a report from a host node, it notes the multicast group that the host node wants to join and the port on the router where the node is located. Any multicast packets belonging to that multicast group are then forwarded by the router from the port. If a particular port on the router has no nodes that want to be members of multicast groups, the router does not send multicast packets from the port. This improves network performance by restricting the multicast packets only to router ports where host nodes are located.

The switch monitors the flow of queries from routers and reports from host nodes to build its own multicast membership lists. It uses the lists to forward multicast packets to only switch ports where there are host nodes that are members of multicast groups. This improves switch performance and network security by restricting the flow of multicast packets to only those switch ports that are connected to host nodes.

The switch maintains its list of multicast groups through an adjustable timeout value, which controls how frequently it expects to see reports from end nodes that want to remain members of multicast groups, and by processing leave requests.

Note

When IGMP snooping is disabled on the switch, all reports are suppressed on a port. The default setting for IGMP snooping on the switch is disabled.

Displaying and Modifying IGMP Snooping Configuration

To display and modify the IGMP Configuration settings, do the following:

1. Select the **Switching** tab.

The Switching Tab is displayed. See Figure 57.

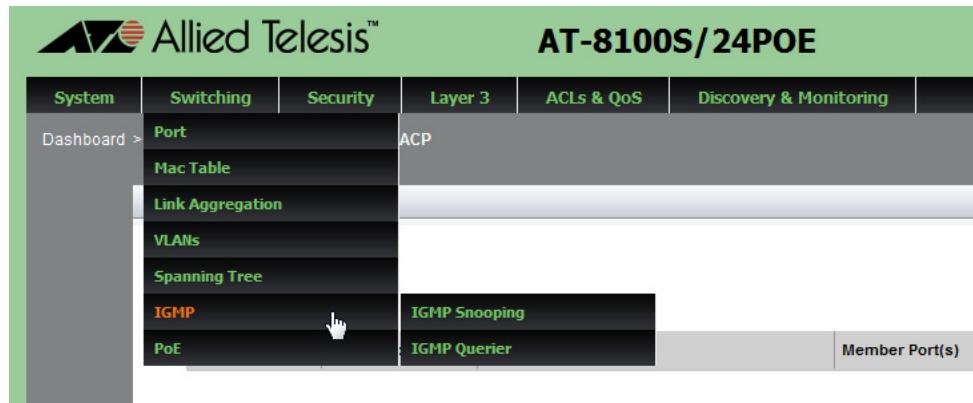


Figure 57. Switching IGMP Tab

2. Select **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

The IGMP Snooping Configuration page is displayed. See Figure 58 on page 162.

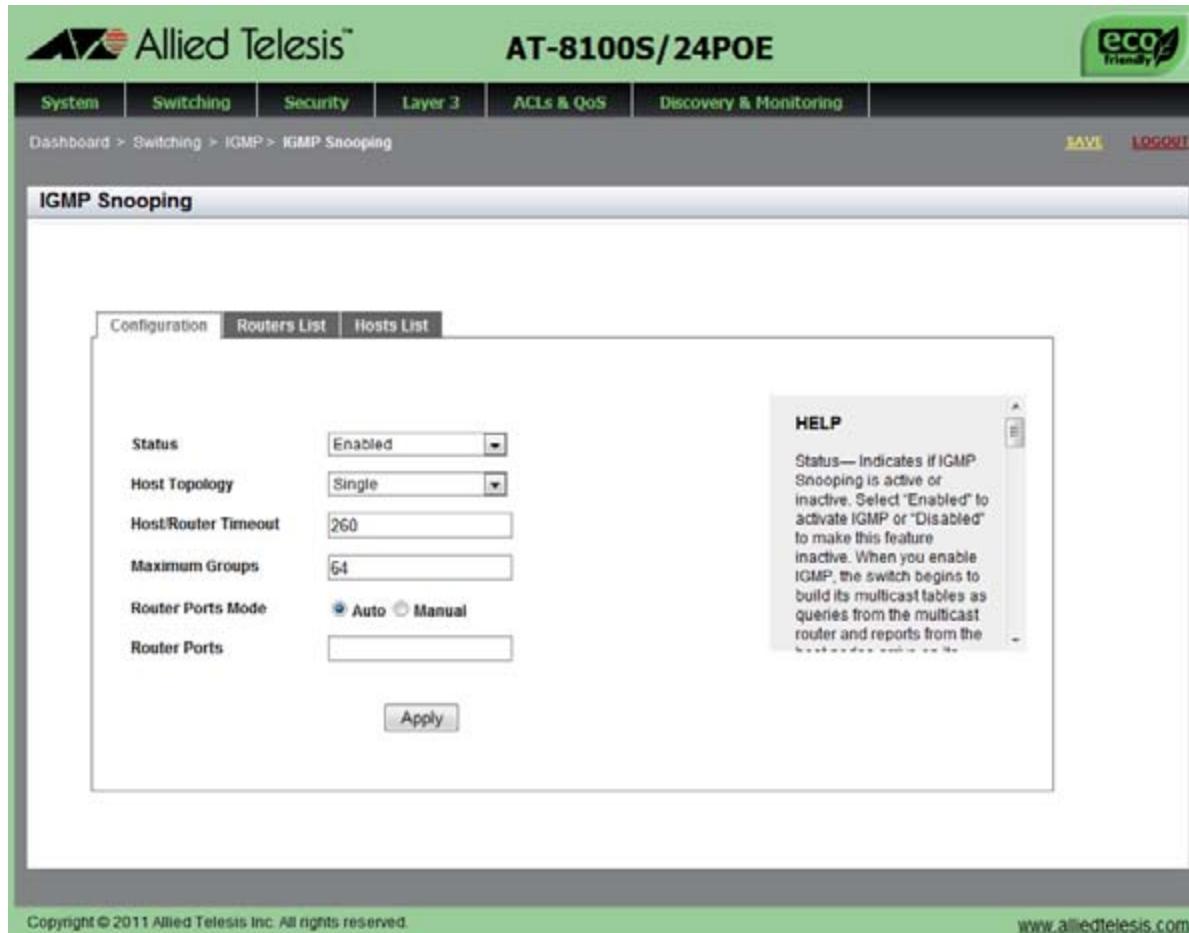


Figure 58. IGMP Snooping Page with Configuration Tab

3. Change the following settings as needed:

- Status**— Enable or disable IGMP Snooping. When you enable IGMP, the switch begins to build its multicast tables as queries from the multicast router and reports from the host nodes arrive on its ports. When you disable IGMP, the switch floods the multicast packets on all of the ports except the port that received the packet.
- Host Topology**— Specify the IGMP host topology. Choose between “Single” and “Multiple.” Select “Single” when the switch has one-host-node per port. Select “Multiple” when the switch has more than one host-node per port. By default, the switch is set to “Single.”
- Host/Router Timeout**— Specify the host/router time in seconds that the switch times out when it finds inactive host nodes and multicast routers. The range is from 0 to 86,400 seconds (24 hours). The default is 260 seconds. Setting the timeout to zero (0) disables the timer.

Maximum Groups— Specify the maximum number of multicast addresses the switch is allowed to learn. The range is 0 to 255 multicast addresses. The default is 64.

Router Ports Mode— Check a radio button to select the router ports mode. Choose from the following:

Auto: Specifies the switch to automatically detect ports that are connected to multicast routers.

Manual: Specifies the switch that you manually specify ports that are connected to multicast routers.

Router Ports— Specify the port ID of a port that is connected to a multicast router. You can enter a port ID in this field only when the Router Ports Mode is “Manual.”

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Disabling IGMP Snooping

To disable the IGMP Configuration on the switch, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 57 on page 161.

2. Select **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 58 on page 162.

3. Use the pull-down menu next to the **Status** field to select “Disabled.”

When you disable IGMP snooping, the switch floods the multicast packets on all of the ports except those that receive the packets.

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Displaying the Routers List

To display the IGMP Routers List, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 57 on page 161.

2. Select **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 58 on page 162.

3. Click the **Routers List** tab.

The Routers List page is displayed. See Figure 59.

VLAN Id	Port Id	Router Ip	Time To Expiry
1	Port 1	10.4.8.1	180 seconds

Figure 59. IGMP Snooping Page with Routers List Tab

The following settings are displayed:

- VLAN ID**— Indicates the ID number of the VLAN of the router port.
- Port ID**— Indicates the port that a multicast router is connected to. If the switch learned a router on a port trunk, the trunk ID number instead of a port number is displayed.
- Router IP**— Indicates the IP address of the multicast router.

- **Time to Expiry**— Indicates the number of seconds remaining before the switch times out a multicast router if there is no further IGMP query from it.

Clearing the Routers List

To clear the group membership on the IGMP Routers List, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 57 on page 161.

2. Select **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 58 on page 162.

3. Click the **Routers List** tab.

The IGMP Snooping page with the Routers List tab selected is displayed. See Figure 59 on page 165.

4. Click **Clear group membership** to remove all multicast router ports in the list.

Removing all multicast router ports also activates auto-detect.

Displaying the Hosts List

To display the IGMP Hosts List, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 57 on page 161.

2. Select **IGMP** and then move the cursor to the right to select **IGMP Snooping**.

The IGMP Snooping page is displayed with the Configuration tab selected by default. See Figure 58 on page 162.

3. Click the **Hosts List** tab.

The Hosts List page is displayed. See Figure 60.

The screenshot shows the Allied Telesis AT-8100S/24POE web interface. The top navigation bar includes tabs for System, Switching (which is selected), Security, Layer 3, ACLs & QoS, and Discovery & Monitoring. The main content area is titled 'IGMP Snooping' and shows a table with one entry:

Group Address	VLAN Id	Port Id	Host IP	IGMP Version	Time To Expiry
01:00:5e:00:00:fb	1	Port 3	10.4.17.62	V2	228 seconds

At the bottom of the page, there is a copyright notice: 'Copyright © 2011 Allied Telesis Inc. All rights reserved.' and a website link: 'www.alliedtelesis.com'.

Figure 60. IGMP Snooping Page with Hosts List Tab

The following settings are displayed:

- Group Address**— Indicates the multicast address of the group.
- VLAN ID**— Indicates the VLAN ID of the host node.
- Port ID**— Indicates the port of the host node. If the host node is on a port trunk, this field displays the trunk ID number instead of the port number.
- Host IP**— Indicates the IP address of the host node.

- IGMP Version**— Indicates the IGMP versions used by the host node.
- Time to Expiry**— Indicates the number of seconds remaining before the host node is timed out if it does not send an IGMP report.

Chapter 14

IGMP Snooping Querier

This chapter provides a brief description of IGMP Snooping Querier and explains how to set this feature on the switch. See the following sections:

- “Overview” on page 172
- “Guidelines” on page 176
- “Displaying IGMP Snooping Querier” on page 177
- “Modifying IGMP Snooping Query Interval” on page 179

For more information about IGMP, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- IGMP Snooping Querier
- IGMP Snooping Querier Commands

Overview

Multicast routers are an essential part of IP multicasting. They send out queries to the network nodes to determine group memberships, route the multicast packets across networks, and maintain lists of the multicast groups and the ports where group members are located.

IGMP snooping querier can be used in place of multicast routers in situations where IP multicasting is restricted to a single LAN, without the need for routing. This feature enables the switch to mimic a multicast router by sending out general IGMP queries to the host nodes.

IGMP snooping querier supports IGMP version 1, version 2, and version 3. By default, the switch sends version 2 messages. If it receives version 1 messages from any of the nodes, the switch sends version 1 queries. If the switch receives version 3 messages, all nodes respond with version 3 messages. By default, the interval at which the querier sends out IGMP querier reports is 125 seconds. The switch reverts to version 2 queries if, after 255 seconds, no additional version 1 or version 3 messages are received.

The switch must have an IP address to add to the queries as its source address. In addition, the address must be a member of the same network as the host nodes and the multicasting source. You assign an IP address to the switch by creating a routing interface in the VLAN. Then apply the IP address to the VLAN where it sends its queries, to enable IGMP snooping querier on the VLAN. Allied Telesis recommends using the Default VLAN which has a VID of 1.

IGMP snooping querier must be used in conjunction with IGMP snooping. Activate IGMP snooping on all of the switches in the LAN, including the switches running the IGMP snooping querier. The switches use IGMP snooping to monitor the responses of the host nodes to the general IGMP queries sent by the IGMP snooping querier. From the responses, they create lists of ports that have host nodes that want to join the various multicast groups and forward the multicast packets to only those ports.

Figure 61 on page 173 provides an example of IGMP snooping querier on a LAN. It consists of a single switch with one VLAN, the Default VLAN. Both IGMP snooping and IGMP snooping querier are enabled on the switch. You assign a routing interface to the VLAN, with an IP address that belongs to the same subnet as the multicast source and the host nodes.

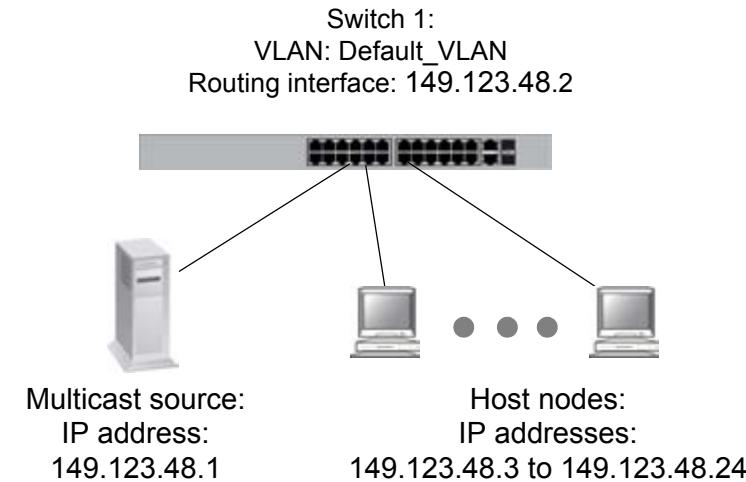


Figure 61. IGMP Snooping Querier with One Querier

Table 3 lists the switch settings that are illustrated in Figure 61.

Table 3. IGMP Snooping Querier with One Querier

Switch	Routing Address	IGMP Snooping	IGMP Snooping Querier	Querier Status
1	149.123.48.2	Enabled	Enabled	Active

Assigning Multiple Queriers

IGMP snooping querier supports multiple queriers. A total of three queriers are supported, one active querier and up to two standby queriers. The active querier is the querier with the lowest IP address. The standby querier has the second lowest IP address and the switch with the highest IP address is the second standby querier.

The difference between the active and standby queriers is that only the active querier registers IGMP reports. A standby querier does not update its MAC tables, so IGMP reports are not registered on the switch.

When you assign multiple queriers to a LAN, the software must decide which is the active querier and which is the standby querier. This task falls to a switch in the network that has IGMP snooping enabled, but IGMP snooping querier disabled. Consequently, a LAN with multiple queriers requires this extra switch.

For example, to assign two queriers to a network, you need three switches. First, enable IGMP snooping on all three switches. Then enable IGMP snooping querier on two switches, for this example, switches 1 and 3. Switch 2 determines which of the querier-enabled switches has the lowest IP address and deems that switch the active querier. The switch

with the second lowest IP address is made the standby querier, again by switch 2. In the case where there are three queriers, the switch in the network with IGMP snooping enabled and IGMP querier disabled determines the standby querier and then the second standby querier by comparing their IP addresses.

The following example consists of a LAN with three switches. See Figure 62. IGMP snooping is enabled on all three switches. However, IGMP snooping querier is enabled on switches 1 and 3. Switch 2 determines that switch 1 has the lowest IP routing address and forwards all multicast packets to switch 1, making switch 1 the active querier. Switch 3 becomes the standby querier in case switch 1 stops transmitting query packets.

Note

Switches 1 and 3 are only sending queriers. Neither switch detects nor displays an opposing querier.

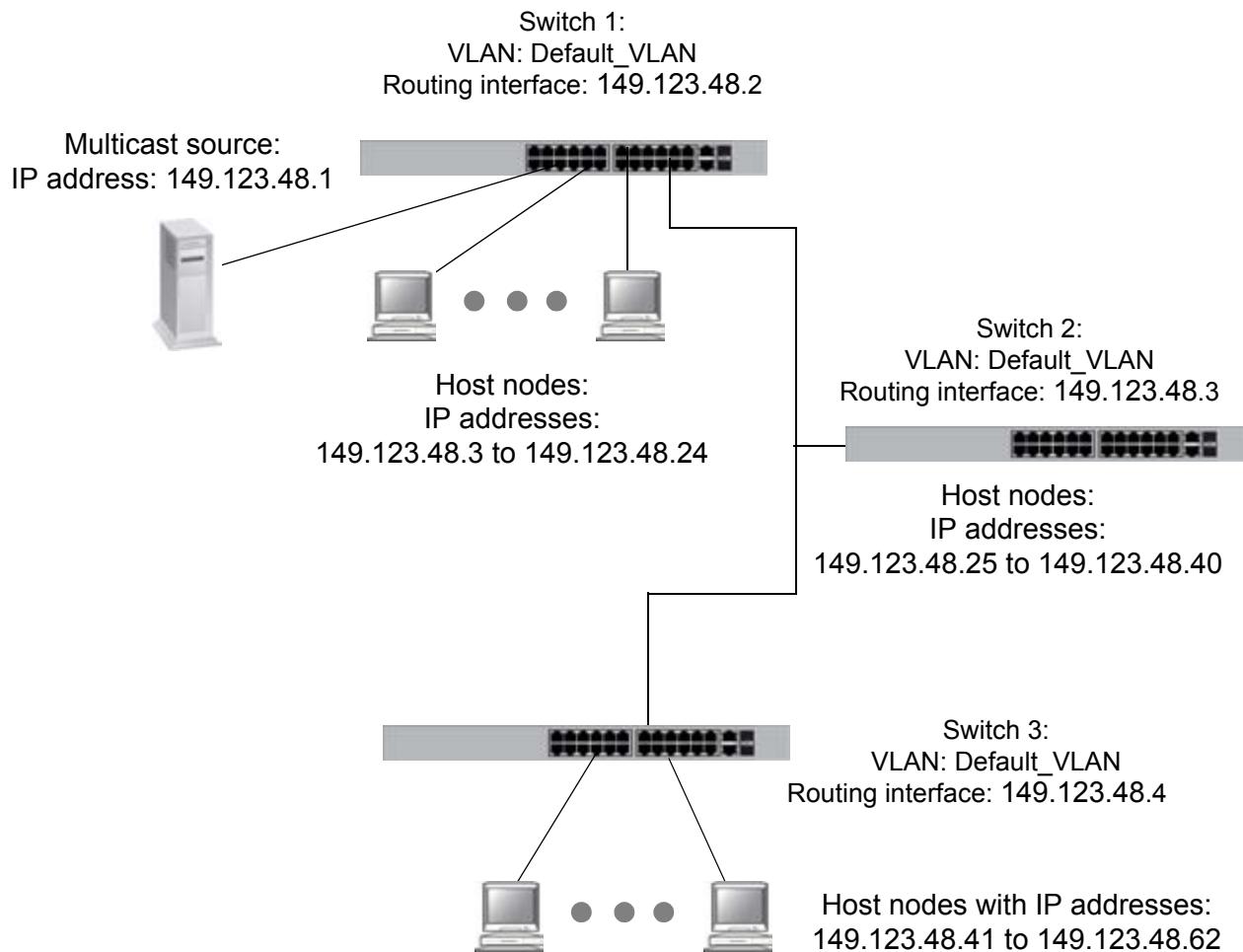


Figure 62. IGMP Snooping Querier with Two Queriers

Table 4 lists the switch settings that are illustrated in Figure 62.

Table 4. IGMP Snooping Querier with Two Queriers

Switch	Routing Address	IGMP Snooping	IGMP Snooping Querier	Querier Status
1	149.123.48.2	Enabled	Enabled	Active
2	149.123.48.3	Enabled	Disabled	None
3	149.123.48.4	Enabled	Enabled	Standby

Guidelines

The guidelines for IGMP snooping querier are listed here:

- ❑ The network can have only one LAN.
- ❑ The network cannot have any multicast routers.
- ❑ IGMP snooping must be enabled on the switch.
- ❑ IGMP snooping querier should be enabled on only one switch. Other switches in the LAN should use IGMP snooping.
- ❑ IGMP snooping querier must be applied to the VLAN on which the queries are to be sent.
- ❑ The VLAN must be assigned a routing interface with an IP address that is a member of the same network as the host nodes and the source node of the multicast packets. The switch adds the IP address to the queries as its source address.
- ❑ If you want to add or remove ports from the VLAN after activating IGMP snooping querier, you must disable IGMP snooping querier, modify the VLAN, and then enable it again.
- ❑ The switch supports IGMP versions 1, 2, and 3. The switch normally sends just version 2 messages. If it receives a version 1 message, it sends version 1 messages on all of the ports. If the switch does not receive any further version 1 messages for 400 seconds, the switch reverts to sending version 2 messages.
- ❑ If the switch receives a query either from a multicast router or from another switch with IGMP snooping querier, it suspends IGMP snooping querier and sends no further queries for 225 seconds. If the switch does not receive any further queries, it reactivates the feature and resumes sending queries.
- ❑ IGMP snooping querier is supported on the base ports and SFP modules.

Displaying IGMP Snooping Querier

To display a list of IGMP Snooping Querier, do the following:

1. Select the **Switching** tab.

The Switching Tab is displayed. See Figure 63.

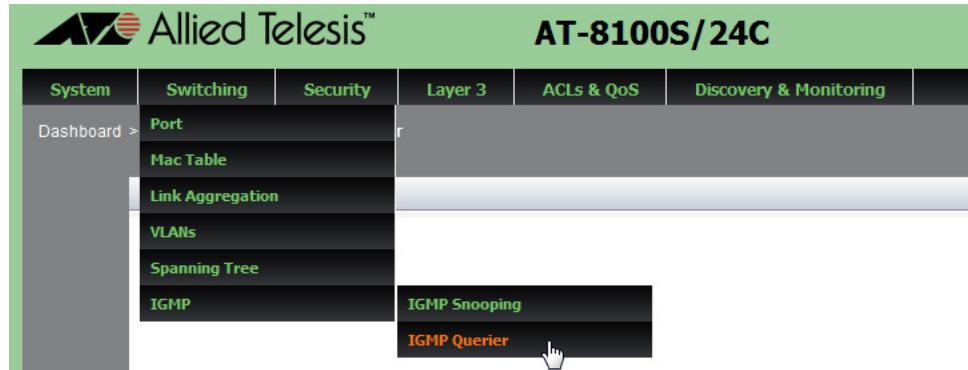


Figure 63. Switching IGMP Tab

2. Select **IGMP** and then move the cursor to the right to select **IGMP Querier**.

The IGMP Snooping Querier page is displayed. See Figure 64.

	VLAN	Query Interval
Delete Edit	1	
Delete Edit	2	
Delete Edit	3	

Figure 64. IGMP Snooping Querier Page

3. The following settings are displayed:

- VLAN**— Indicates the VLAN ID.
- Query Interval**— Indicates the time interval in seconds at which IGMP General Query messages are transmitted.

Modifying IGMP Snooping Query Interval

To modify the value of Query interval, do the following:

1. Select the **Switching** tab.

The Switching Tab is displayed. See Figure 63 on page 177.

2. Select **IGMP** and then move the cursor to the right to select **IGMP Querier**.

The IGMP Snooping Querier page is displayed. See Figure 64 on page 177.

3. From the IGMP Snooping Querier page, click Add or Edit.

The Edit IGMP Snooping Querier page is displayed. See Figure 65.

The screenshot shows the 'Edit IGMP Snooping Querier' page. At the top, the navigation bar includes tabs for System, Switching (which is selected), Security, Layer 3, ACLs & QoS, and Discovery & Monitoring. Below the navigation bar, the page title is 'IGMP Snooping Querier'. The main form contains two input fields: 'VLAN' (set to 'Vlan1') and 'Query Interval' (set to '125'). Below these fields is an 'Apply' button. To the right of the form is a 'HELP' section with the following text: 'Range— The range of query interval is <2 - 18000>sec with the default value being 125 seconds.' At the bottom of the page, there is a copyright notice 'Copyright © 2011 Allied Telesis Inc. All rights reserved.' and a website link 'www.alliedtelesis.com'.

Figure 65. Edit IGMP Snooping Querier Page

4. Enter the following settings as needed:

- VLAN**— Selects the VLAN ID from the pull-down menu.
- Query Interval**— Enter a query interval in seconds. The range is 2 to 18,000. The default is 125 seconds.

5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Chapter 15

Power Over Ethernet (PoE)

This chapter provides brief descriptions of PoE and explains how to change the configuration of a port on the PoE featured switch.

See the following sections:

- “Overview” on page 182
- “Displaying PoE Port Settings” on page 184
- “Modifying PoE Settings on a Port” on page 188

For more information about PoE, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Power Over Ethernet
- Power Over Ethernet Commands

Overview

The AT-8100L/8PoE, AT-8100S/24PoE, and AT-8100S/48PoE switches feature Power over Ethernet (PoE) on the 10/100Base-Tx ports. PoE is used to supply power to network devices over the same twisted pair cables that carry the network traffic.

The main advantage of PoE is that it can make installing a network easier. The selection of a location for a network device is often limited by whether there is a power source nearby. This constraint limits equipment placement or requires the added time and cost of having additional electrical sources installed. However, with PoE, you can install PoE-compatible devices wherever they are needed without having to worry about whether there is power source nearby.

Power Sourcing Equipment (PSE)

A device that provides PoE to other network devices is referred to as power sourcing equipment (PSE). The AT-8100L/8PoE, AT-8100S/24PoE, and AT-8100S/48PoE switches are PSE devices providing DC power to the network cable and functioning as a central power source for other network devices.

Powered Device (PD)

A device that receives power from a PSE device is called a *powered device* (PD). Examples include wireless access points, IP phones, webcams, and even other Ethernet switches.

PD Classes

PDs are grouped into five classes. The classes are based on the amount of power that PDs require. The AT-8100 PoE switches support all five classes listed in Table 5.

Table 5. IEEE Powered Device Classes

Class	Maximum Power Output from a Switch Port	Power Ranges of the PDs
0	15.4W	0.44W to 12.95W
1	4.0W	0.44W to 3.84W
2	7.0W	3.84W to 6.49W
3	15.4W	6.49W to 12.95W
4	34.2W	25.5W to 38.9W

Port Prioritization

As long as the total power requirements of the PDs is less than the total available power of the switch, it can supply power to all of the PDs. However, when the PD power requirements exceed the total available power, the switch denies power to some ports based on a process called port prioritization.

The ports on the PoE switch are assigned to one of three priority levels. These levels and descriptions are listed in Table 6.

Table 6. PoE Port Priorities

Priority Level	Description
Critical	This is the highest priority level. Ports set to the Critical level are guaranteed to receive power before any of the ports assigned to the other priority levels.
High	Ports set to the High level receive power only when all the ports assigned to the Critical level are already receiving power.
Low	This is the lowest priority level. Ports set to the Low level receive power only when all the ports assigned to the Critical and High levels are already receiving power. This level is the default setting.

Without enough power to support all the ports set to the same priority level at one time, the switch provides power to the ports based on the port number, in ascending order. For example, when all of the ports in the switch are set to the low priority level and the power requirements are exceeded on the switch, port 1 has the highest priority level, port 2 has the next highest priority level and so forth.

Displaying PoE Port Settings

To display a list of the PoE port settings, do the following:

Note

The PoE pull-down menu item appears only when you are accessing a PoE featured switch.

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 66.

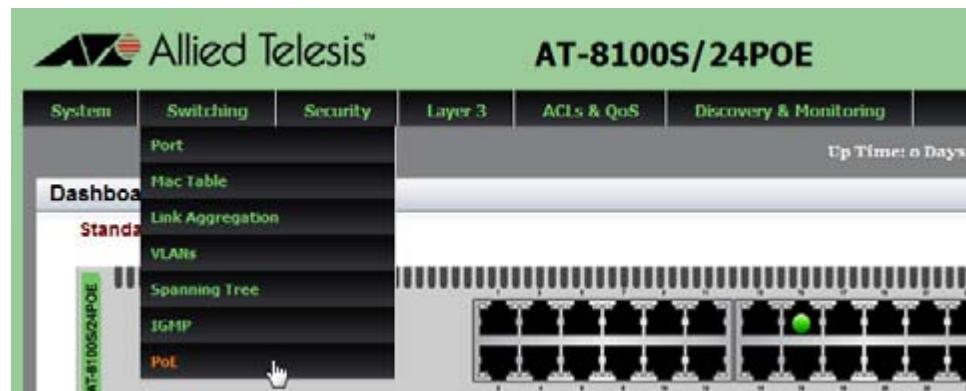


Figure 66. Switching Tab

2. From the **Switching** tab, select **PoE**.

A list of PoE settings on the ports is displayed. See Figure 67 on page 185.

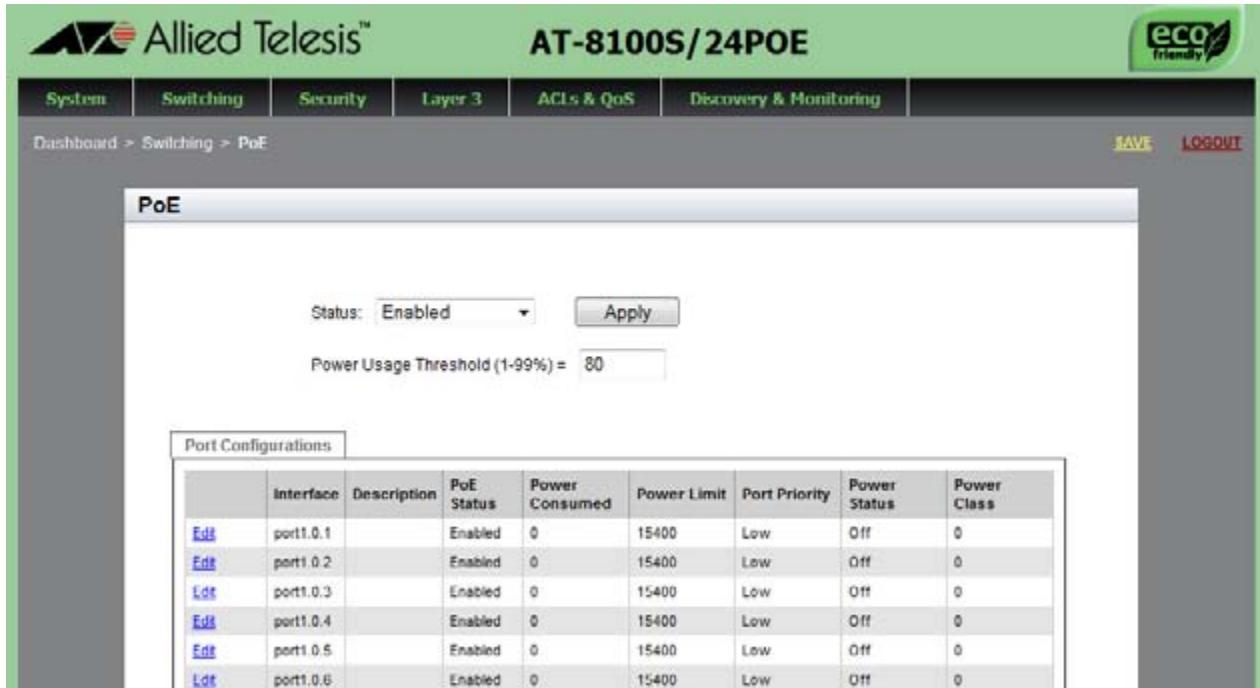


Figure 67. PoE Port List Page

The following fields are displayed:

- Status**— Enable or disable PoE on the ports globally. By default, PoE is enabled on all ports.

Note

This status does not indicate that the PoE status of all the ports is the same. To find out the PoE status, you must examine the PoE status for a port individually.

- Power Usage Threshold**— Indicates the power usage threshold in a percentage of the switch's total available power. The range is 1 to 99%.
- Interface**— Indicates the port ID.
- Description**— Indicates the description of the port.
- PoE Status**— Indicates if PoE for the port is enabled or disabled. By default, PoE is enabled for all the ports on the switch.
- Power Consumed**— Indicates the power consumption in milliwatts (mW) for the port.
- Power Limit**— Indicates the power limit in milliwatts (mW) on the port.
- Port Priority**— Indicates the port priority: Low, High, or Critical. For more details, see "Port Prioritization" on page 183.

- **Power Status**— Indicates if a powered device that is connected to the port is powered on or off. When no powered device is connected to the port, indicates Off.
- **Power Class**— Indicates the class of the connected PD. The switch automatically detects which class the connected PD belongs to. For more details, see “PD Classes” on page 182.

Modifying PoE Settings Globally

To modify PoE settings on the switch, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 66 on page 184.

2. From the **Switching** tab, select **PoE**.

Note

The PoE pull-down menu item appears only when you are accessing an AT-8100 PoE switch.

The PoE setting page is displayed. See Figure 67 on page 185.

3. Change the following settings as needed:

- Status**— Enable or disable PoE globally for all the ports on the switch. Change this field when you want to change the PoE status for all the ports all at once.
- Power Threshold**— Set the power usage threshold in a percentage of the switch's total available power. The range is 1 to 99%. By default, the power threshold is 80% of the total available power of the switch.

Note

The power threshold value is used to monitor power consumption on the switch. You can configure the switch with an SNMP server to notify you when the switch reaches power consumption at the specified level. To configure an SNMP server, you must use the AlliedWare Plus™ Command Line Interface (CLI). See the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User's Guide*.

4. Click **Apply**.

5. Click **SAVE** to save your changes to the startup configuration file.

Modifying PoE Settings on a Port

To display a list of the IPv4 interfaces, do the following:

1. Select the **Switching** tab.

The Switching tab is displayed. See Figure 68.

2. From the **Switching** tab, select **PoE**.

A list of PoE settings on the ports is displayed. See Figure 67 on page 185.

3. From the PoE page, click Edit next to the port number that you want to modify.

The following page is displayed. See Figure 68.

The screenshot shows the 'Modify Port PoE Settings' page of the Allied Telesis AT-8100S/24POE web interface. The page has the following fields:

- Interface:** port1.0.4
- PoE port status:** Enabled
- PoE device Description:** (empty text input field)
- PoE port Power Limit (4000-30000):** 15400
- PoE legacy device:** No
- PoE port Priority:** Low
- Apply:** (button)

A help panel on the right provides the following descriptions:

- Interface**—Indicates the port ID.
- PoE Port Status**—Select Enabled or Disabled. The default setting is Enabled.
- PoE Device Description**—Enter the description of the PoE device that is connected to the port. The description can contain up to 256 alphanumeric characters. Spaces and special characters are allowed. Note: The description will only show first 32 characters.
- PoE Port Power Limit**—Enter the

At the bottom of the page, there is a copyright notice: Copyright © 2011 Allied Telesis Inc. All rights reserved. and a website link: www.alliedtelesis.com

Figure 68. Modify Port PoE Settings Page

4. Change the following fields as needed:

- Interface**— Indicates the port ID.
- PoE Port Status**— Enable or disable the PoE port status.
- PoE Device Description**— Enter the description of the PoE device that is connected to the port. The description can contain up to 256 alphanumeric characters. Spaces and special characters are allowed.
- PoE Port Power Limit (4000 ~ 30000)**— Enter the power limit in milliwatts (mW) that the switch provides to a device connected to the port.
- PoE Legacy Device**— Select “Yes” to allow the switch to supply power to a device that is connected to the port even if the device is a legacy PD. Select “No” to not allow the switch to supply power if a device that is connected to the port is a legacy PD. By default, the PoE switch does not supply power to legacy PDs.

Legacy PDs are PoE devices that were designed before the IEEE 802.3af and IEEE 802.3at PoE standards were finalized.

- PoE Port Priority**— Select the PoE port priority from Low, High or Critical. For more details, see “Port Prioritization” on page 183.

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Chapter 16

MAC Address-based Port Security

This chapter provides a brief description of MAC address-based port security and explains how to set this feature on the switch. See the following sections:

- “Overview” on page 192
- “Displaying the MAC Address-based Port Security Settings” on page 194
- “Modifying the MAC Address-based Port Security Settings” on page 196
- “Disabling MAC Address-based Port Security Settings” on page 198

For more information about MAC address-based security, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- MAC Address-based Port Security
- MAC Address-based Port Security Commands

Overview

This feature lets you control access to the ports on the switch based on the source MAC addresses of the network devices. You specify the maximum number of source MAC addresses that ports can learn. Ports that learn their maximum number of addresses discard packets that have new, unknown addresses, preventing access to the switch by any additional devices.

For example, if you configure port 3 on the switch to learn five source MAC addresses, the port learns up to five address and forwards the ingress packets of the devices that belong to those addresses. If the port receives ingress packets that have source MAC addresses other than the five it has already learned, it discards those packets to prevent the devices from passing traffic through the switch.

Static Versus Dynamic Addresses

The MAC addresses that the ports learn can be stored as either static or dynamic addresses in the MAC address table in the switch. Ports that store the addresses as static addresses do not learn new addresses after they have learned their maximum number. In contrast, ports that store the addresses as dynamic addresses can learn new addresses when addresses are timed out from the table by the switch. The addresses are aged out according to the aging time of the MAC address table.

Intrusion Actions

The intrusion actions define what the switch does when ports that have learned their maximum number of MAC addresses receive packets that have unknown source MAC addresses. Intrusion actions are also called violation actions. The possible settings are:

- Protect— Ports discard those frames that have unknown MAC addresses. No other action is taken. For example, if port 14 is configured to learn 18 addresses, it starts to discard packets with unknown source MAC addresses after learning 18 MAC addresses.
- Restrict— This is the same as the protect action, except that the switch sends SNMP traps when the ports discard frames. For example, if port 12 is configured to learn two addresses, the switch sends a trap every time the port, after learning two addresses, discards a packet that has an unknown MAC address.
- Shutdown— The switch disables the ports and sends SNMP traps. For example, if port 5 is configured to learn three MAC addresses, it is disabled by the switch to prevent it from forwarding any further traffic if it receives a packet with an unknown source MAC address, after learning three addresses. The switch also sends an SNMP trap.

Guidelines Here are the guidelines to MAC address-based port security:

- The filtering of a packet occurs on the ingress port, not on the egress port.
- You cannot use MAC address-based port security and 802.1x port-based access control on the same port. To specify a port as an Authenticator or Supplicant in 802.1x port-based access control, you must remove MAC address-based port security.
- MAC address-based port security is not supported on the optional GBIC, SFP, or XFP modules.

Displaying the MAC Address-based Port Security Settings

To display the MAC address-based port security settings, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69.

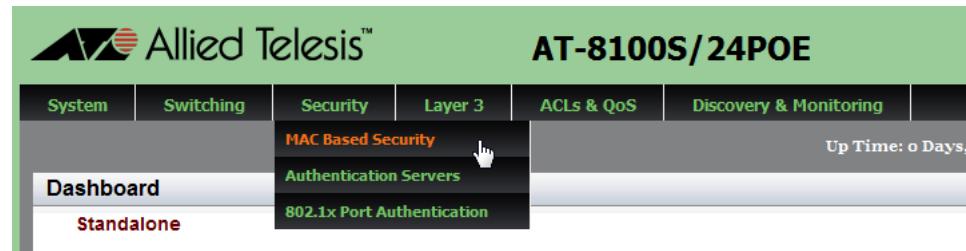


Figure 69. Security Tab

2. From the Security tab, select **MAC Based Security**.

The MAC Based Port Security page is displayed. See Figure 70.

The screenshot shows the MAC Based Port Security page. The top navigation bar includes tabs for System, Switching, Security, Layer 3, ACLs & QoS, and Discovery & Monitoring. The Security tab is selected. The main content area shows the 'MAC Based Port Security' table with 10 rows, each representing a port (port1.0.1 to port1.0.10). The table columns are: Interface, MAC Security, Aging, MAX MACs, and Violation Action. All ports are currently set to 'Disabled' for MAC Security and 'No' for Aging. The 'MAX MACs' column shows values from 0 to 1. The 'Violation Action' column shows 'Protect' for all ports. There are 'Edit' links next to each port ID in the first column. A green 'eco friendly' logo is in the top right corner. Navigation links 'Dashboard > Security > MAC Based Port Security' are at the top left, and 'SAVE' and 'LOGOUT' buttons are at the top right.

MAC Based Port Security					
	Interface	MAC Security	Aging	MAX MACs	Violation Action
Edit	port1.0.1	Disabled	No	0	Protect
Edit	port1.0.2	Disabled	No	0	Protect
Edit	port1.0.3	Disabled	No	0	Protect
Edit	port1.0.4	Disabled	No	0	Protect
Edit	port1.0.5	Disabled	No	0	Protect
Edit	port1.0.6	Disabled	No	0	Protect
Edit	port1.0.7	Disabled	No	0	Protect
Edit	port1.0.8	Disabled	No	0	Protect
Edit	port1.0.9	Disabled	No	0	Protect
Edit	port1.0.10	Disabled	No	0	Protect

Figure 70. MAC Based Port Security Page

The following fields are displayed:

- Interface**— Indicates the port ID.
- MAC Security**— Indicates MAC address-based security is either “Enabled” or “Disabled” on a port. By default, this setting is disabled.

- Aging**— Indicates one of the following:

Yes: Saves the source MAC addresses as dynamic addresses in the MAC address table.

No: Saves the source MAC addresses as static addresses in the MAC address table. This is the default setting.

- MAX MACs**— Indicates maximum number of dynamic MAC addresses the port is permitted to learn. The range is 0 to 255. By default, this field is set to 0.

- Violation Action**— Indicates one of the following actions:

Protect: Discards invalid frames. This is the default setting.

Restrict: Discards invalid frames and sends SNMP traps.

Disable: Sends SNMP traps and disables the port.

Modifying the MAC Address-based Port Security Settings

To the modify the MAC address-based port security settings, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69 on page 194.

2. From the Security tab, select **MAC Based Security**.

The MAC Based Port Security page is displayed. See Figure 70 on page 194.

3. Click Edit next to the port that you want to modify.

The Modify MAC Based Port Security page is displayed. See Figure 71.

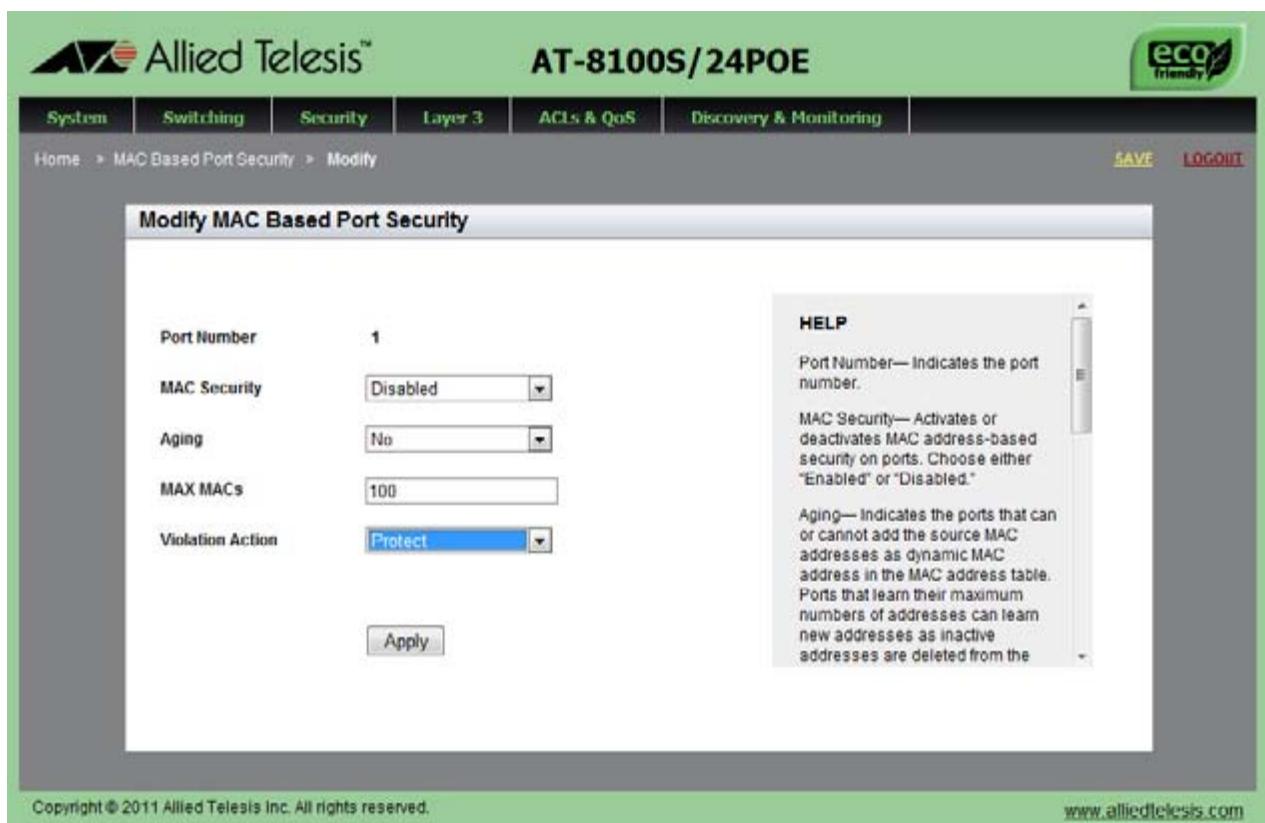


Figure 71. Modify MAC Based Port Security Page

4. Change the following settings as needed:

- Interface**— Indicates the port number.
- MAC Security**— Select between “Enabled” and “Disabled” to activate or deactivate MAC address-based security on the port.
- Aging**— Select how the switch saves source MAC addresses to the MAC address table. Choose from the following options:
 - Yes**: Saves the source MAC addresses as dynamic addresses in the MAC address table.
 - No**: Saves the source MAC addresses as static addresses in the MAC address table.
- MAX MACs**— Enter the maximum number of source MAC addresses that the switch can learn and store for the port. The range is 0 to 255. The default is 100 addresses.
- Violation Action**— Select the intrusion action of the port. Choose from the following:
 - Protect**: Discards invalid frames.
 - Restrict**: Discards invalid frames and sends SNMP traps.
 - Disable**: Sends SNMP traps and disables the port.

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Disabling MAC Address-based Port Security Settings

To deactivate MAC address-based port security settings, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69 on page 194.

2. From the Security tab, select **MAC Based Security**.

The MAC Based Port Security page is displayed. See Figure 70 on page 194.

3. Click Edit next to the port that you want to remove.

The Modify MAC Based Port Security page is displayed. See Figure 71 on page 196.

4. Use the pull-down menu next to the **MAC Security** field and select "Disabled."

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

RADIUS and TACACS+ Clients

This chapter provides a brief description of both the RADIUS and TACACS+ clients and explains how to configure these clients on the switch.

See the following sections:

- “Overview” on page 200
- “Configuring RADIUS for Remote Manager Authentication” on page 203
- “Configuring TACACS+ for Remote Manager Authentication” on page 208
- “Deleting an Authentication Server” on page 213

For more information about the authentication server features, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- RADIUS and TACACS+ Clients
- RADIUS and TACACS+ Client Commands

Overview

The switch has RADIUS and TACACS+ clients for remote authentication. Here are the features that use remote authentication:

- ❑ 802.1x port-based network access control. This feature lets you increase network security by requiring that network users log on with user names and passwords before the switch forwards their packets. This feature is described in Chapter 18, “802.1x Port-based Network Access” on page 215.
- ❑ Remote manager accounts. This feature lets you add manager accounts to the switch by transferring the authenticating task from the switch to an authentication server on your network. Accounts that the switch authenticates are called local accounts. This feature is described in “Managing Local User Accounts” on page 53.

The RADIUS client supports both features, but the TACACS+ client supports only the remote manager accounts feature. Here are the guidelines:

- ❑ Only one client can be active on the switch at a time.
- ❑ If you want to use only the remote manager account feature, you can use either RADIUS or TACACS+ because both clients support that feature.
- ❑ If you want to use 802.1x port-based network access control, you have to use the RADIUS client because the TACACS+ client does not support that feature.

Remote Manager Accounts

The switch comes with one local manager account. The account is referred to as a local account because the switch authenticates the user name and password when a manager uses the account to log on. If the user name and password are valid, the switch allows the individual to access its management software. Otherwise, it cancels the login to prevent unauthorized access.

There are two ways to add more manager accounts. The first way is to create additional local accounts. For more information about local accounts, see “Managing Local User Accounts” on page 53.

The second way to add more accounts is with a RADIUS or TACACS+ authentication server on your network. With either authentication method, the authentication of the user names and passwords of the manager accounts is performed by one or more authentication servers. The switch forwards the information to the servers when managers log on.

The following steps illustrate the authentication process that occurs between the switch and an authentication server when a manager logs on:

1. The switch uses its RADIUS or TACACS+ client to transmit the user name and password to an authentication server on the network.
2. The server checks to see if the user name and password are valid.
3. If the combination is valid, the authentication server notifies the switch, which completes the login process, allowing the manager access to its management software.
4. If the user name and password are invalid, the authentication protocol server notifies the switch, which cancels the login.

Accounting Information

RADIUS and TACACS+ also provides a way to monitor usage by login users. You can configure the switch to send a start accounting message at the beginning of a session and a stop accounting message at the end of the session to an authentication sever.

Configuring RADIUS and TACACS+

To authenticate using a RADIUS or TACACS+ server, you must configure remote manager authentication and add authentication servers that the switch can access.

You can configure up to three servers each for the RADIUS and TACACS+ features. However, only one authentication method, either RADIUS or TACACS+, at a time.

To configure remote manager authentication and add authentication servers, choose from the following procedures:

- “Configuring RADIUS for Remote Manager Authentication” on page 203
- “Configuring TACACS+ for Remote Manager Authentication” on page 208

Placing RADIUS and TACACS+ Servers in the Client’s List

When a user logs on to the switch, the authentication client polls the servers for authentication information in the order in which they are listed in the client. The order that you add a server determines its order on the client. For instance, the first server that you add becomes Server 1, the second server that you add becomes Server 2, and the third server that you add becomes Server 3.

When you remove a server from the switch, the place holder is retained. For example, you make the following assignments:

- Server 1 has an IP address of 192.168.10.11
- Server 2 has an IP address of 192.168.10.12
- Server 3 has an IP address of 192.168.10.13

When you delete Server 1, the server with an IP address of 192.168.10.12 remains Server 2; the server with an IP address of 192.168.10.13 remains Server 3. As a result, the next server that you add to the switch becomes Server 1.

Configuring RADIUS for Remote Manager Authentication

To configure remote manager authentication using RADIUS and add RADIUS servers to the switch, perform the following:

- “Configuring Remote Manager Authentication Using RADIUS” on page 203
- “Adding a RADIUS Server” on page 206

Configuring Remote Manager Authentication Using RADIUS

To configure the RADIUS server, do the following:

1. Select the **Security** tab.
The Security tab is displayed. See Figure 69 on page 194.
2. From the Security tab, select **Authentication Servers**.

The Authentication Server Configuration page with the RADIUS tab selected is displayed. See Figure 72 on page 204.

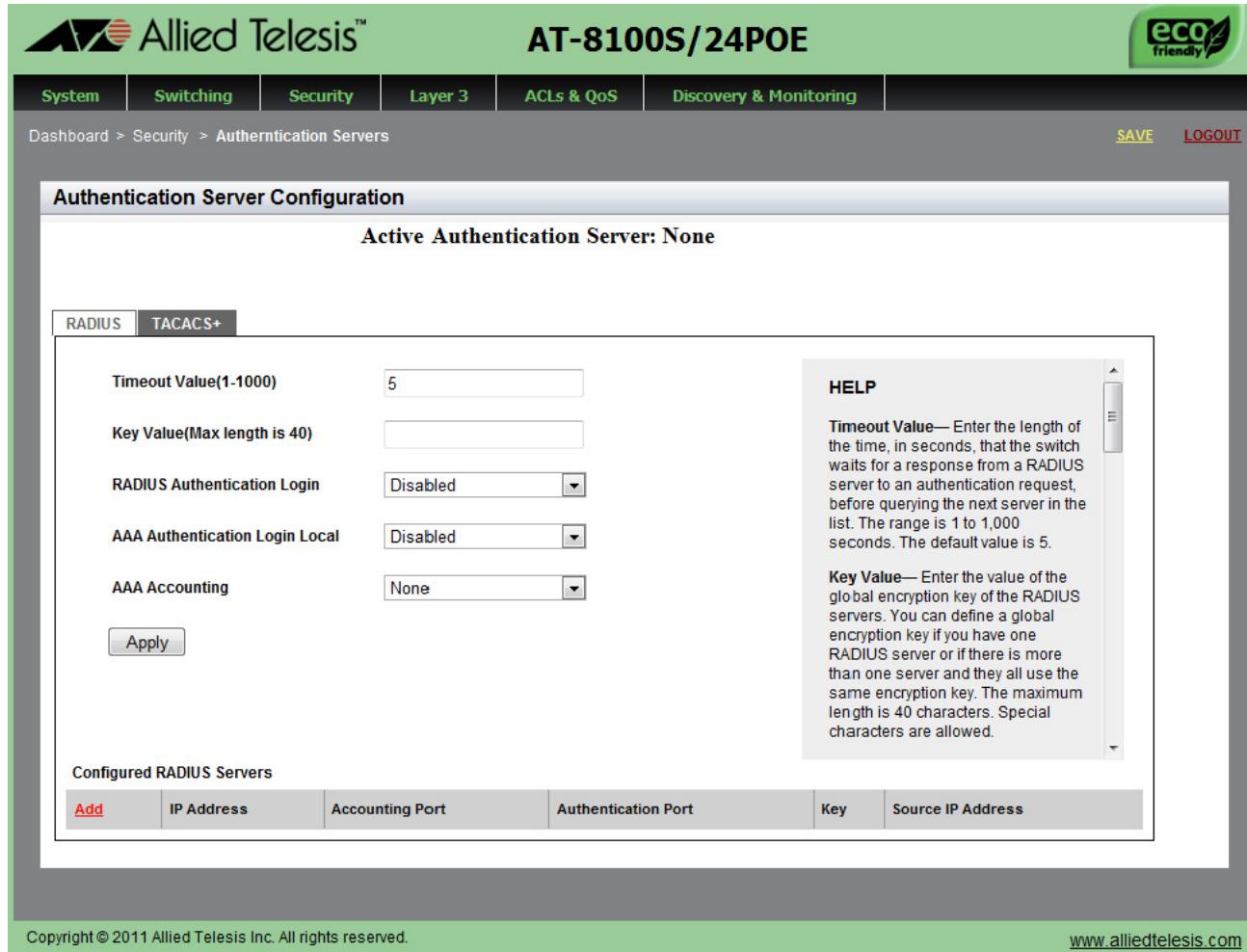


Figure 72. Authentication Server Configuration Page with RADIUS Tab

3. Change the following fields as needed:

- Timeout Value**— Enter the length of the time, in seconds, that the switch waits for a response from a RADIUS server to an authentication request, before querying the next server in the list. The range is 1 to 1,000 seconds. The default value is 5 seconds.
- Key Value**— Enter the value of the global encryption key of the RADIUS servers. You can define a global encryption key if you have one RADIUS server or if there is more than one server and they all use the same encryption key. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

**Caution**

To define two or three servers that use different encryption keys, do not enter a global encryption key value on this web page. Instead, define the individual keys when you add the IP addresses of the servers to the client on the RADIUS Server Configuration Page. See “Adding a RADIUS Server” on page 206.

RADIUS Authentication Login— Enable or disable RADIUS to authenticate user login. Choose from the following:

Enabled: The RADIUS servers authenticate user login.

Disabled: The RADIUS servers do not authenticate user login. Authentication is attempted using the user name and password combinations specified on the User Management page and using the USERNAME command in the CLI.

AAA Authentication Login Local— Enable or disable RADIUS to authenticate user login in combination with local manager accounts. Choose from the following:

Enabled: The RADIUS servers authenticate the user login. When any RADIUS server is not available, authentication is attempted using the user name and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Disabled: The RADIUS servers do not authenticate user login. Authentication is attempted using the user name and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Note

For additional information about the User Management page, see “Managing Local User Accounts” on page 53. For more information about the USERNAME command, see “Local Manager Accounts” in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*.

AAA Accounting— Select a RADIUS accounting setting. Choose from the following:

Start-Stop: Indicates that a start accounting message is sent at the beginning of a session and a stop accounting message is sent at the end of the session.

Stop-Only: Indicates a stop accounting message is sent at the end of the session.

None: Indicates that sending accounting messages is disabled.

4. Click **Apply**.

The Active Authentication Server field shown on the upper middle of the page indicates “RADIUS.”

5. Click **SAVE** to save your changes to the startup configuration file.

Adding a RADIUS Server

To add a RADIUS server, do the following:

6. Click **Add** near the RADIUS server list.

The Authentication Server Configuration page with the RADIUS tab selected is displayed. See Figure 73.

The screenshot shows the 'RADIUS Server Add' configuration page. The page has a header with the Allied Telesis logo, model name 'AT-8100S/24POE', and an 'eco friendly' badge. The navigation bar includes 'System', 'Switching', 'Security', 'Layer 3', 'ACLs & QoS', 'Discovery & Monitoring', 'Dashboard', 'Security', 'Authentication Servers', and 'Add'. There are 'SAVE' and 'LOGOUT' buttons. The main form has fields for 'IP Address', 'Accounting Port' (set to 1813), 'Authentication Port' (set to 1812), 'Key', and 'Source IP Address of Radius Packet' (set to 'Vlan1'). A 'Help' section on the right provides descriptions for these fields. At the bottom, there is a copyright notice and a website link.

Figure 73. Radius Add Page

7. Enter the following fields as needed:

- IP Address**— Enter the IP address of a RADIUS server on the network. The IP address must be in the following IPv4 format: xxx.xxx.xxx.xxx.

- Accounting Port**— Specify the UDP destination port for RADIUS accounting requests. If you select 0, the server is not used for accounting. The default UDP port for accounting is 1813.
- Authentication Port**— Specify the UDP destination port for RADIUS authentication requests. If you select 0, the server is not used for authentication. The default UDP port for authentication is 1812.
- Key**— Enter the encryption key for RADIUS communications between the switch and RADIUS server. The key must match the encryption key used by the RADIUS server. The maximum length is 39 characters. Special characters are allowed, but spaces are not permitted.

8. Click **Save**.
9. Click **SAVE** to save your changes to the startup configuration file.

Configuring TACACS+ for Remote Manager Authentication

To configure remote manager authentication using TACACS+ and add TACACS+ servers to the switch, perform the following:

- “Configuring Remote Manager Authentication Using TACACS+” on page 208
- “Adding a TACACS+ Server” on page 211

Configuring Remote Manager Authentication Using TACACS+

To configure a TACACS+ server, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69 on page 194.

2. From the Security tab, select **Authentication Servers**.

The Authentication Server Configuration page is displayed. See Figure 72 on page 204.

3. Click the **TACACS+** tab.

The Authentication Server Configuration Page with the TACACS+ tab is displayed. See Figure 74 on page 209.

The screenshot shows the 'Authentication Server Configuration' page for the AT-8100S/24POE switch. The 'TACACS+' tab is selected. The configuration section includes fields for 'Timeout Value(1-1000)' (set to 5), 'Key Value(Max length is 40)' (empty), and several AAA authentication and accounting dropdowns (all set to 'Disabled' or 'None'). A 'HELP' panel on the right provides detailed descriptions for these fields. Below the configuration is a table for 'Configured TACACS+ Servers' with columns for 'Add', 'IP Address', and 'Key'.

Figure 74. Authentication Server Configuration Page with TACACS+ Tab

4. Change the following fields as needed:

- Timeout Value**— Enter the length of the time, in seconds, that the switch waits for a response from a TACACS+ server to an authentication request, before querying the next server in the list. The range is 1 to 1,000 seconds. The default value is 5.
- Key Value**— Enter the value of the global encryption key of the TACACS+ servers. You can define a global encryption key if you have one TACACS+ server or if there is more than one server and they all use the same encryption key. The maximum length is 40 characters. Special characters are allowed, but spaces are not permitted.

**Caution**

To define two or three servers that use different encryption keys, do not enter a global encryption key value on this web page. Instead, define the individual keys when you add the IP addresses of the servers to the switch on the TACACS+ Add page. See “Adding a RADIUS Server” on page 206.

- TACACS+ Authentication Login**— Enable or disable TACACS+ to authenticate user login. Choose from the following:

Enabled: The TACACS+ servers authenticate user login.

Disabled: The TACACS+ servers do not authenticate user login. Authentication is attempted using the user name and password combinations specified on the User Management page and using the USERNAME command in the CLI.

- AAA Authentication Login Local**— Enable or disable TACACS+ to authenticate user login in combination with local manager accounts. Choose from the following:

Enabled: The TACACS+ servers authenticate user login. When any TACACS+ server is not available, authentication is attempted using the user name and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Disabled: The TACACS+ servers do not authenticate user login. Authentication is attempted using the user name and password combinations specified on the User Management page and using the USERNAME command in the CLI.

Note

For additional information about the User Management page, see “Managing Local User Accounts” on page 53. For more information about the USERNAME command, see Chapter 88: Local Manager Accounts in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*.

- AAA Authentication Enable**— Enable or disable TACACS+ to authenticate users requesting the Privileged Exec mode. Choose from the following:

Enabled: The TACACS+ determines whether users can access the Privileged EXEC level using TACACS+ enable password.

Disabled: The TACACS+ servers do not use its enable password. Authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.

- AAA Authentication Enable Local**— Enable or disable TACACS+ to authenticate users requesting the Privileged Exec mode. Choose from the following:

Enabled: The TACACS+ determines whether users can access the Privileged EXEC level using TACACS+ enable password. When any TACACS+ server is not available, authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.

Disabled: The TACACS+ servers do not use its enable password. Authentication is attempted using the password specified using the ENABLE PASSWORD command in the CLI.

- AAA Accounting**— Select a TACACS+ accounting setting. Choose from the following:

Start-Stop: Indicates that a start accounting message is sent at the beginning of a session and a stop accounting message is sent at the end of the session.

Stop-Only: Indicates a stop accounting message is sent at the end of the session.

None: Indicates that sending accounting messages is disabled.

5. Click **Apply**.

The Active Authentication Server field shown on the upper middle of the page indicates “TACACS.”

6. Click **SAVE** to save your changes to the startup configuration file.

Adding a TACACS+ Server

To add a TACACS+ server, do the following:

1. Click **Add** at the bottom of the page.

The TACACS+ Add page is displayed. See Figure 75 on page 212.

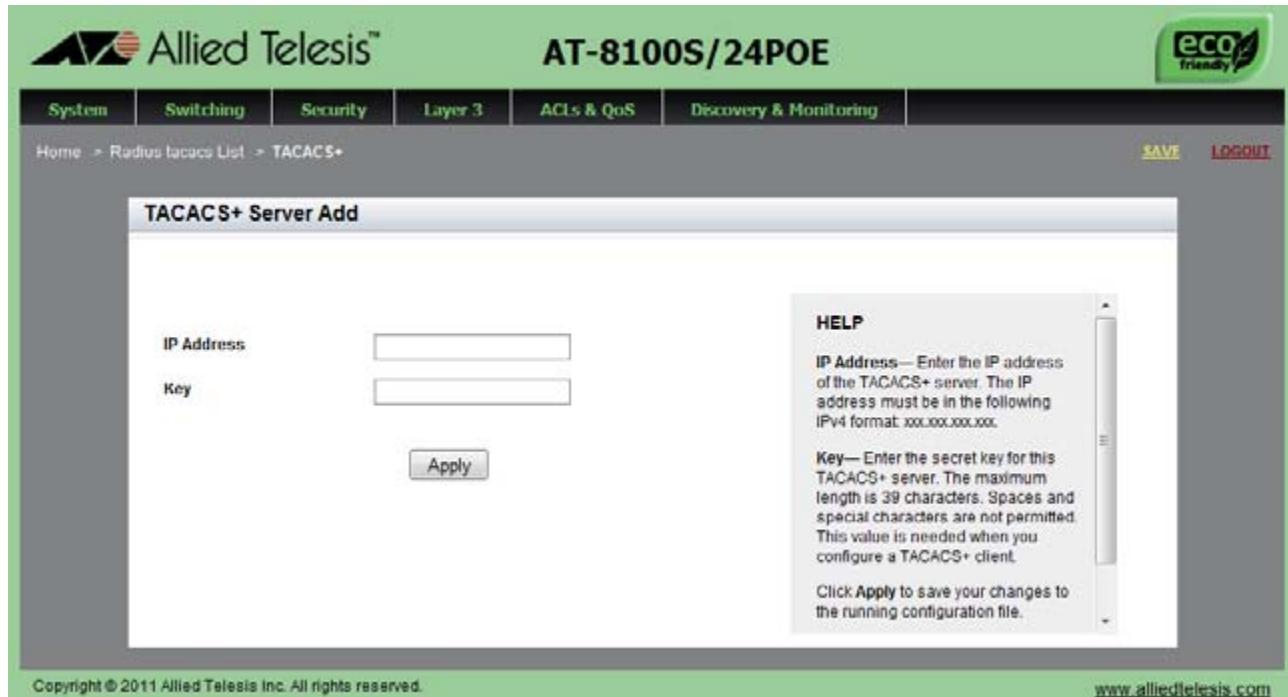


Figure 75. TACACS+ Add Page

2. Enter the following settings:
 - IP Address**—Enter the IP address of the TACACS+ server. The IP address must be in the following IPv4 format: xxx.xxx.xxx.xxx.
 - Key**—Enter the encryption key for TACACS+ communications between the switch and TACACS+ server. The key must match the encryption key used by the TACACS+ server. The maximum length is 39 characters. Special characters are allowed, but spaces are not permitted.
3. Click **Save**.
4. Click **SAVE** to save your changes to the startup configuration file.

Deleting an Authentication Server

To delete either an TACACS+ or RADIUS authentication server, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69 on page 194.

2. From the Security tab, select **Authentication Servers**.

The Authentication Server Configuration page is displayed. See Figure 72 on page 204.

3. Click either the TACACS+ or the RADIUS tab, depending on the type of server you want to delete.

4. Click **Delete** next to the server that you want to delete.

Chapter 18

802.1x Port-based Network Access

This chapter provides a brief description of the 802.1x Port-based Authentication feature and explains how to enable this feature on the switch, and specify authentication on a port.

See the following sections:

- “Overview” on page 216
- “Enabling 802.1x Port-based Authentication on the Switch” on page 221
- “Configuring 802.1x Port-based Authentication” on page 222
- “Disabling 802.1x Port-based Authentication on the Switch” on page 227
- “Disabling 802.1x Port-based Authentication on a Port” on page 228

For more information about the 802.1x features, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- 802.1x Port-based Network Access Control
- 802.1x Port-based Network Access Control Commands

Overview

The 802.1x port-based network access control feature lets you control who can send traffic through and receive traffic from the individual switch ports. The switch does not allow an end node to send or receive traffic through a port until the user of the node has been authenticated by a RADIUS server.

This port-security feature is used to prevent unauthorized individuals from connecting a computer to a switch port or using an unattended workstation to access your network resources. Only those users designated as valid network users on a RADIUS server are permitted to use the switch to access the network.

This port security method uses the RADIUS authentication protocol. To use the 802.1x port-based network access control feature, you must configure RADIUS and add RADIUS servers to the switch. For more information about RADIUS and its configuration, see Chapter 17, “RADIUS and TACACS+ Clients” on page 199.

Note

RADIUS with Extensible Authentication Protocol (EAP) extensions is the only supported authentication protocol for 802.1x port-based network access control. This feature is not supported with the TACACS+ authentication protocol.

The switch does not authenticate any end nodes connected to its ports. Its function is to act as an intermediary between the end nodes or users and the RADIUS authentication server during the authentication process.

Port Roles

Part of the task to implementing this feature is specifying the roles of the ports on the switch. The roles are listed here:

None Role:

Switch ports in the none role do not participate in port-based access control. They forward traffic without authenticating the clients of the network devices. This is the default setting for the switch ports.

Note

A RADIUS authentication server cannot authenticate itself and must communicate with the switch through a port that is set to the none role.

Authenticator Role:

The authenticator role activates port access control on a port. Ports in this role do not forward network traffic to or from network devices until the clients are authenticated by a RADIUS server. The authenticator role is appropriate when you want the switch to authenticate the clients of network devices before they can use the network.

Figure 76 illustrates the none role and authentication role.

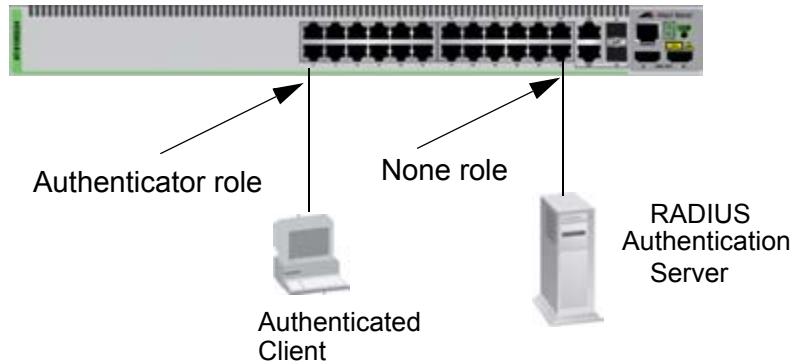


Figure 76. Example of Port Roles

Operating Modes

Authenticator ports have three modes:

Single host mode

An authenticator port set to the single host mode permits only one supplicant to log on and forwards only the traffic of that supplicant. After one supplicant has logged on, the port discards packets from any other supplicant.

In Figure 77, port 6 is an authenticator port set to the single host mode. It permits only one supplicant to log on and forwards the traffic of only that supplicant.

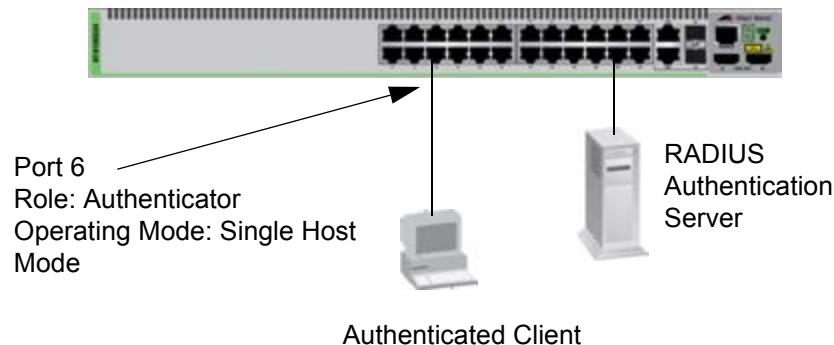


Figure 77. Single Host Mode

- **Multiple host mode**

This mode permits multiple clients on an authenticator port. An authenticator mode forwards packets from all clients once one client has successfully logged on. This mode is typically used in situations where you want to add 802.1x port-based network access control to a switch port that is supporting multiple clients, but do not want to create individual accounts for all the clients on the RADIUS server.

This is referred to as “piggy-backing.” After one client has successfully logged, the port permits the other clients to piggy-back onto the initial client’s log on, so that they can forward packets through the port without being authenticated.

Figure 78 is an example of this mode. Port 6 is connected to an Ethernet hub or non-802.1x-compliant switch, which in turn is connected to several supplicants. The switch does not forward the client traffic until one of the clients logs on. Afterwards, it forwards the traffic of all the clients.

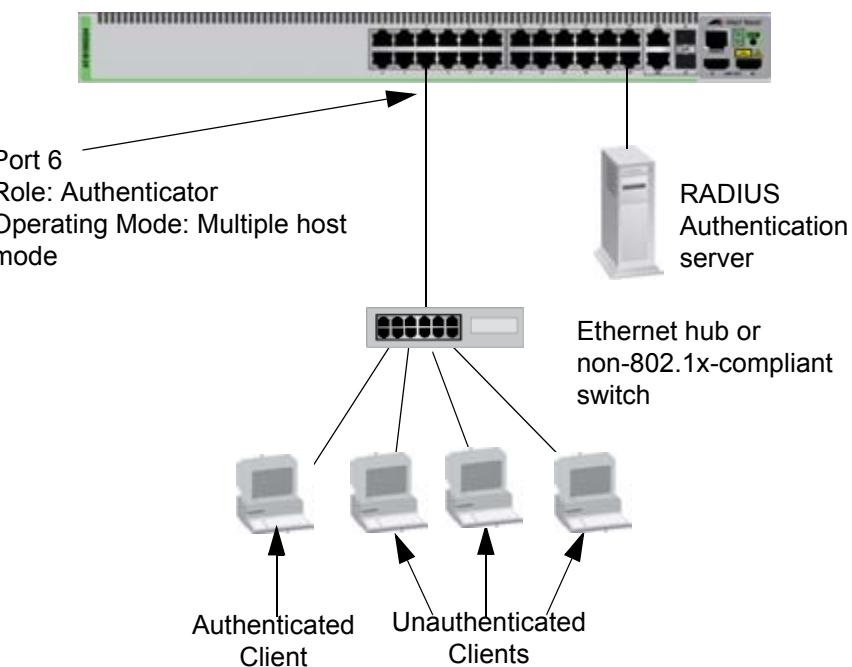


Figure 78. Multiple Host Operating Mode

- **Multiple supplicant mode**

This mode authenticates all the clients on an authenticator port. This mode is appropriate in situations where an authenticator port is supporting more than one client and you want all clients to be authenticated. An authenticator port in this mode can support up to a maximum of 320 clients, with a total maximum of 0 per switch.

An example of this authenticator operating mode is illustrated in Figure 79 on page 219. The clients are connected to a hub or non-802.1x-compliant switch which is connected to an authenticator port on the switch. If the authenticator port is set to the 802.1x authentication method, the clients must provide their username and password combinations before they can forward traffic through the switch.

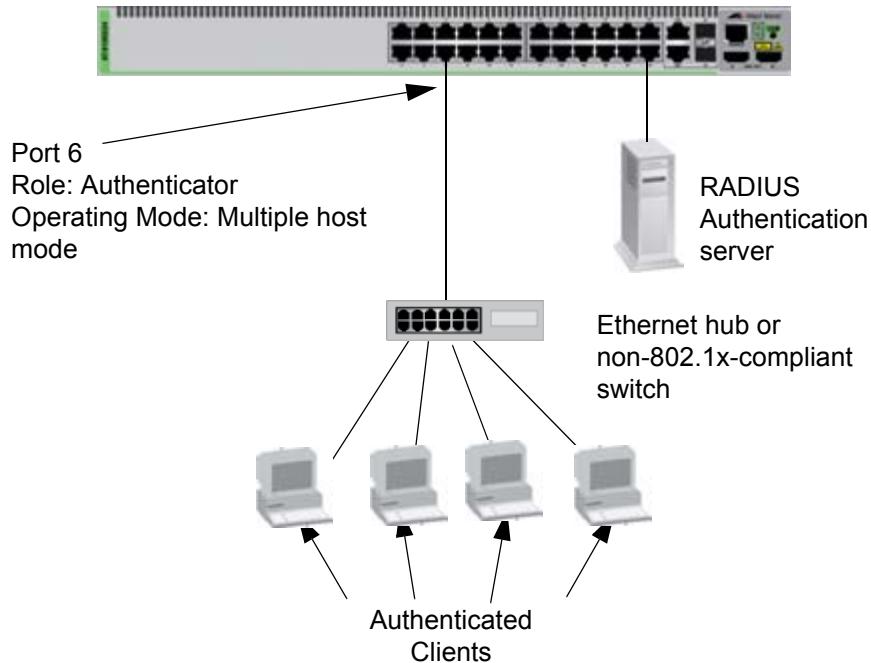


Figure 79. Multiple Supplicant Mode

Dynamic VLAN Assignments

With 802.1x port-based network access control, you can link a username and password combination or MAC address to a specific VLAN so that the switch automatically moves the port to the appropriate VLAN when a client logs on. This frees the network manager from having to reconfigure VLANs as end users access the network from different points or where the same workstation is used by different individuals at different times.

To use this feature, you have to enter a VLAN identifier, along with other information, when you create a client account on the RADIUS server. The server passes the identifier to the switch when a user logs on with a valid username and password combination or MAC address, depending on the authentication method.

How the switch responds when it receives VLAN information during the authentication process can differ depending on the operating mode of the authenticator port.

Guest VLAN

An authenticator port in the unauthorized state typically accepts and transmits only 802.1x packets while waiting to authenticate a client. However, you can specify an authenticator port to be a member of a Guest VLAN when no authenticated client is logged on. Any guest user using the port is not required to log on and has full access to the resources of the Guest VLAN.

If the switch receives 802.1x packets on the port, signalling that an authenticated client is logging on, it moves the port to its predefined VLAN and places it in the unauthorized state. The port remains in the unauthorized state until the log on process between the authenticated client and the RADIUS server is completed. When the authenticated client logs off, the port automatically returns to the Guest VLAN.

Note

The Guest VLAN feature is only supported on an authenticator port in the Single operating mode.

Enabling 802.1x Port-based Authentication on the Switch

To enable the 802.1x port-based Authentication feature on a switch, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69 on page 194.

2. From the Security tab, select **802.1x Port Authentication**.

The 802.1x Authentication page is displayed. See Figure 80.

The screenshot shows the '802.1x Authentication' configuration page. At the top, there is a status dropdown set to 'Disabled' with an 'Apply' button. Below this is a table with 12 rows, each representing a port (port1.0.1 to port1.0.12) and its current 'Port Role' set to 'None'. Each row has an 'Edit' link next to the port number.

	Interface	Port Role
Edit	port1.0.1	None
Edit	port1.0.2	None
Edit	port1.0.3	None
Edit	port1.0.4	None
Edit	port1.0.5	None
Edit	port1.0.6	None
Edit	port1.0.7	None
Edit	port1.0.8	None
Edit	port1.0.9	None
Edit	port1.0.10	None
Edit	port1.0.11	None
Edit	port1.0.12	None

Figure 80. 802.1x Authentication Page

3. Use the pull-down menu next to the Status field to select “Enabled.”
The default setting is “Disabled.”
4. Click **Apply**.
5. Click **SAVE** to save your changes to the startup configuration file.

Configuring 802.1x Port-based Authentication

To set 802.1x port authentication on a port, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69 on page 194.

2. From the Security tab, select **802.1x Port Authentication**.

The 802.1x Authentication page is displayed. See Figure 80 on page 221.

3. Click Edit next to the port that you want to modify.

The Modify 802.1x Authentication page is displayed. See Figure 81.

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 81. Modify 802.1x Authentication Page

4. Use the pull-down menu next to the **Port Role** field to select "Authenticator."

The Modify 802.1x Authentication page "Authenticator" expands. See Figure 82 on page 223.

Modify 802.1x Authentication

Interface	port1.0.9	Port Role
Authentication Mode	Unauthorized	
Timeouts		
Quiet-period	60	
Tx-period	30	
Reauth-period	3600	
Supplicant-timeout	30	
Server-timeout	30	
<input checked="" type="checkbox"/> Re-authentication		
Number of Re-auth Requests	2	
<input checked="" type="checkbox"/> Port Control Direction	Both	
<input checked="" type="checkbox"/> Dynamic VLAN Creation		
Type	Multi	
Guest VLAN		
Host Mode	Single-Host	
<input checked="" type="checkbox"/> Mac Authentication		
<input checked="" type="checkbox"/> Re-auth Learning		

HELP

Port Id— Indicates the port number.

Port Role— Indicates that you've selected the port as an Authenticator.

Authentication Mode— Indicates the authentication mode. Choose from the following:

- **Unauthorized**: Sets the port to the 802.1X authenticator role, in the unauthorized state. Although the port is in the authenticator role, the switch blocks all authentication on the port. If you set all the ports on the switch to this setting, then no clients can log on and forward packets through them.
- **Force-authorized**: Sets port to the 802.1X authenticator role, in the force-authorized state. A port in the force-authorized state transitions to the authorized state without any authentication exchanges required. The port transmits and receives traffic normally without 802.1X-based authentication of the clients.
- **Auto**: Sets the port to the 802.1X port-based authenticator role. A port in this state begins in the unauthorized state, forwarding only EAPOL frames, until a client has logged on successfully.

Timeouts:

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 82. Modify 802.1x Authentication Page Expanded

5. Modify the following fields as needed:

- Interface**— Indicates the port ID.
- Port Role**— Indicates that you've selected the port as an Authenticator.

- Authentication Mode**— Select the authentication mode. Choose from the following:

Unauthorized: Sets the port in the unauthorized state.

Although the port is in the authenticator role, the switch blocks all authentication on the port. If you set all the ports on the switch to this setting, then no clients can log on and forward packets through them.

Force-authorized: Sets port in the force-authorized state. A port in the force-authorized state transitions to the authorized state without any authentication exchanges required. The port transmits and receives traffic normally without 802.1X-based authentication of the clients.

Auto: Sets the port active in the authenticator role. A port in this state begins in the unauthorized state, forwarding only authentication frames, until a client has logged on successfully.

- Timeouts**

The following fields set the timers for this feature:

- Quiet Period**— Enter the number of seconds that an authenticator port remains in the quiet state following a failed authentication exchange with a client. The range is 0 to 65,535 seconds. The default value is 60 seconds.
- Tx-period**— Enter the number of seconds that an authenticator port waits for a response to an EAP-request/identity frame from a client before retransmitting the request. The range is 1 to 65,535 seconds. The default value is 30 seconds.
- Reauth-period**— Enter the time interval that an authenticator port requires a client to reauthenticate. The range is 1 to 65,535 seconds. The default value is 3,600 seconds.
- Supplicant-timeout**— Enter the retransmission time for the EAP-request frame from the authenticator port. The range is 1 to 600 seconds. The default value is 30 seconds.
- Server-timeout**— Enter the number of seconds the switch waits for a response from the authentication server. The range is 1 to 600 seconds. The default value is 30 seconds.
- Re-authentication**— Check the checkbox to activate reauthentication on the authenticator port. The client periodically reauthenticates according to the time interval set with the Reauth-period timer.
- Number of Re-auth Requests**— Enter the maximum number of times the switch retransmits EAP Request packets to an client before it times out an authentication session. The range is 1 to 10 retransmissions. The default value is 2.

- Port Control Direction**— Select whether the authenticator port that is in the unauthorized state should forward egress broadcast and multicast traffic. Choose from the following:

In: Specifies that the authenticator port in the unauthorized state should forward egress broadcast and multicast traffic and discard the ingress broadcast and multicast traffic. This is the default setting.

Both: Specifies that the authenticator port in the unauthorized state should discard both ingress and egress broadcast and multicast traffic.

- Dynamic VLAN Creation**— Check the checkbox to activate dynamic VLAN assignments of the authenticator port.
- Type**— Select the type of dynamic VLAN assignments. Choose from the following:

Single: Specifies that an authenticator port forwards packets of only those clients that have the same VID as the client who initially logged on.

Multi: Specifies that an authenticator port forwards packets of all clients, regardless of the VIDs in their client accounts on the RADIUS server.

- Guest VLAN**— Select the ID number of a VLAN that is the guest VLAN of an authenticator port. You can select only one VID.
- Host Mode**— Select the operating mode on an authenticator port. Choose from the following:

Single-host: Specifies the single operating mode. An authenticator port set to this mode forwards only those packets from the one client who initially logs on. This is the default setting.

Multi-host: Specifies the multiple host operating mode. An authenticator port set to this mode forwards all packets after one client logs on. This is referred to as piggy-backing.

Multi-suppliant: Specifies the multiple supplicant operating mode. An authenticator port set to this mode requires that all clients log on.

- Mac Authentication**— Check the checkbox to activates MAC address-based authentication on the authenticator port. An authenticator port that uses this type of authentication extracts the source MAC address from the initial frame from a client and automatically sends it as the client's user name and password to the authentication server.

This authentication method does not require 802.1x client software on client nodes.

- Re-Auth Learning**— Select the checkbox to force the port that is using MAC address authentication into the unauthorized state. You may use this setting to reauthenticate the nodes on the authenticator port.

6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Disabling 802.1x Port-based Authentication on the Switch

To disable the 802.1x port-based Authentication feature on a switch, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69 on page 194.

2. From the Security tab, select **802.1x Port Authentication**.

The 802.1x Authentication page with the Status field set to “Enabled” is displayed. See Figure 83.

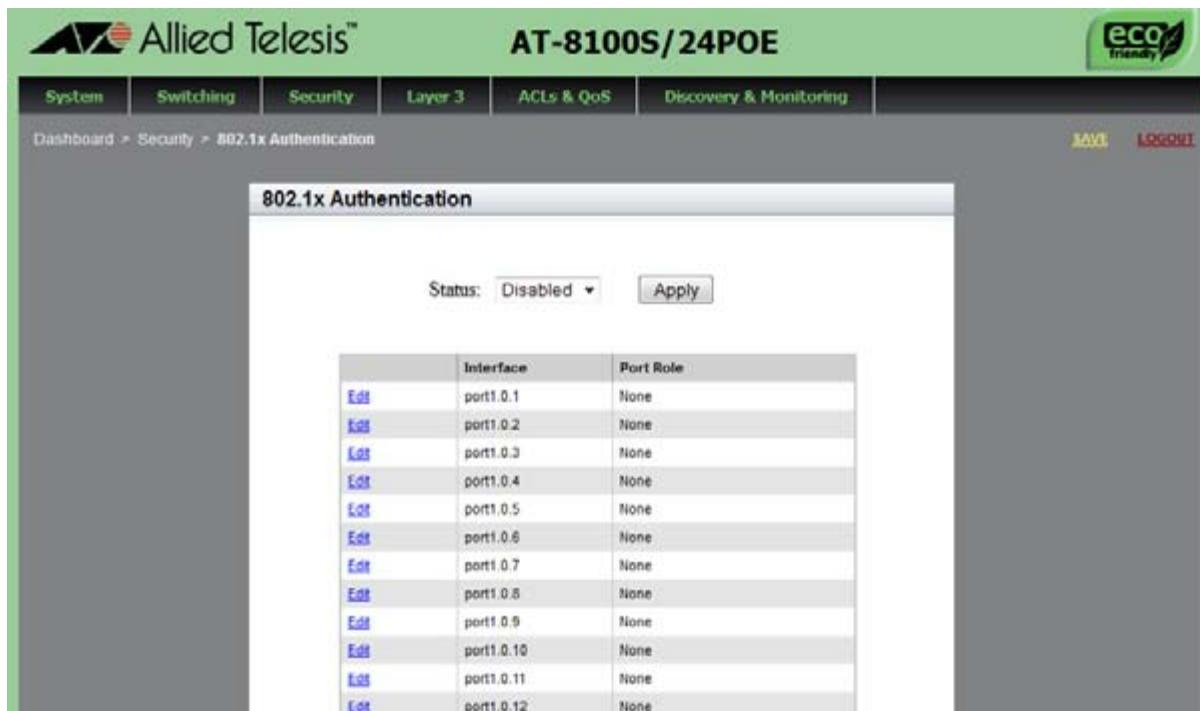


Figure 83. 802.1x Authentication Page with Status Enabled

3. Use the pull-down menu next to the **Status** field to select “Disabled.”
4. Click **Apply**.
5. Click **SAVE** to save your changes to the startup configuration file.

Disabling 802.1x Port-based Authentication on a Port

To disable 802.1x port authentication on a port, do the following:

1. Select the **Security** tab.

The Security tab is displayed. See Figure 69 on page 194.

2. From the Security tab, select **802.1x Port Authentication**.

The 802.1x Authentication page is displayed. See Figure 80 on page 221.

3. Click Edit next to the port that you want to modify.

The Modify 802.1x Authentication page is displayed. See Figure 81 on page 222.

4. Use the pull-down menu next to the **Port Role** field to select “None.”

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Chapter 19

Setting IPv4 and IPv6 Addresses

This chapter provides brief descriptions of management IPv4 and IPv6 addresses and explains how to specify both types of IP addresses on the switch.

See the following sections:

- “Overview” on page 230
- “Displaying IPv4 Interfaces” on page 232
- “Adding an IPv4 Address” on page 234
- “Changing an IPv4 Address” on page 236
- “Deleting an IPv4 Address” on page 238
- “Adding an IPv6 Address” on page 241
- “Changing IPv6 Addresses” on page 243
- “Deleting IPv6 Addresses” on page 245

For more information about the IP management address, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- IPv4 and IPv6 Management Addresses
- IPv4 and IPv6 Management Address Commands

Overview

The management IP address is an IP address that the switch uses to identify itself to other network devices, such as TFTP servers and Telnet clients. The management address can be any IPv4 address, or an IPv6 address for some features, that is assigned to a VLAN on the switch. The features listed in Table 7 require that the switch is assigned a management IP address.

You can assign an IP address only to a VLAN interface. You can assign one IPv4 address per VLAN. The switch can have as many IPv4 addresses as there are VLANs on the switch. You can assign an IPv6 address to any VLAN; however, you can assign only one IPv6 address to the switch.

You can use an IPv6 address as the management IP address. However, as shown in Table 7, the IPv6 address supports only the TACACS+ client and HTTP clients. To use features that are not supported by the IPv6 address, you must use an IPv4 address as the management IP address.

Note

In the Command Line Interface, there are additional features that require either an IPv4 or IPv6 address.

Table 7. Web Interface Features that Require an IP Management Address

Feature	Description	Supported by IPv4 Address	Supported by IPv6 Address
802.1x port-based network access control	Used for port security.	yes	no
RADIUS client	Used for remote management authentication and for 802.1x port-based network access control.	yes	no
sFlow agent	Used to transmit packet statistics and port counters to an sFlow collector on your network.	yes	no
TACACS+ client	Used for remote management authentication using a TACACS+ server on your network.	yes	yes

Table 7. Web Interface Features that Require an IP Management Address (Continued)

Feature	Description	Supported by IPv4 Address	Supported by IPv6 Address	
HTTP client	Used for a Web browser to bring the AT-8100 Web interface on your network.	yes	yes	
IP Management Guidelines		<p>See the following list for guidelines about assigning a management IPv4 or IPv6 address to the switch:</p> <ul style="list-style-type: none"> <input type="checkbox"/> You can assign one IPv4 address per VLAN. <input type="checkbox"/> Any IPv4 address can be used as the management IP address. <input type="checkbox"/> The switch can have only one IPv6 address. <input type="checkbox"/> The management IPv4 address can be any IPv4 address assigned to a VLAN on the switch. For background information on VLANs, see Chapter 11, "Setting Port-based and Tagged VLANs" on page 139. <input type="checkbox"/> In the AlliedWare Plus™ Version 2.2.4 Web interface, the IPv4 address is assigned as the static address. The Web interface does not support the assignment of an IPv4 address from a DHCP server. When you want to assign an IPv4 address from a DHCP server, see the <i>AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User's Guide</i>. <input type="checkbox"/> An IPv6 address is assigned as the static address. The switch does not support the assignment of an IPv6 address from a DHCP server. <input type="checkbox"/> To assign the default gateway IPv4 address, you must assign it as the static route. For assigning a static route, see Chapter 21, "Setting Static Routes" on page 259. <input type="checkbox"/> To assign the default gateway IPv6 address, you must add it when you assign the management IPv6 address. See Chapter 19, "Adding an IPv6 Address" on page 241. <input type="checkbox"/> The IPv4 management address and the default gateway IPv4 address must be members of the same network. <input type="checkbox"/> The IPv6 management address and the default gateway IPv6 address must be members of the same network. 		

Displaying IPv4 Interfaces

To display a list of the IPv4 interfaces, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 84.

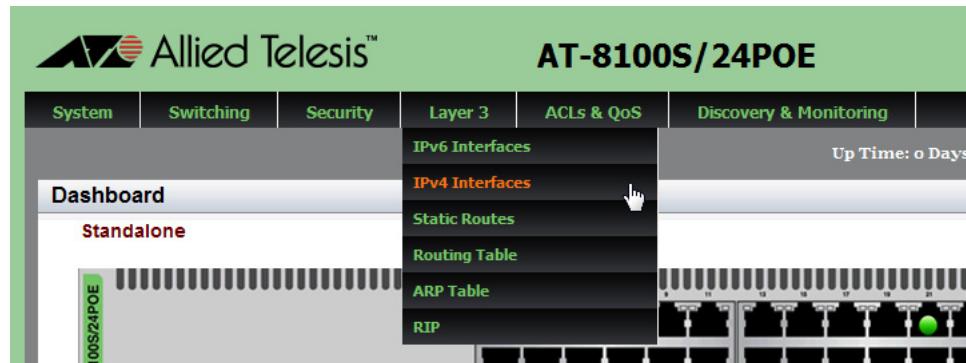


Figure 84. Layer 3 Tab

2. From the **Layer 3** tab, select **IPv4 Interfaces**.

A list of IPv4 interfaces is displayed. See Figure 85.

The screenshot shows the 'IPv4 Interfaces' page under the Layer 3 tab. The top navigation bar includes System, Switching, Security, Layer 3, ACLs & QoS, and Discovery & Monitoring. The 'IPv4 Interfaces' page shows the following table:

	VLAN	IP Address	Subnet Mask	Status
Delete Edit	vlan1-0	192.168.2.1	255.255.255.0	up
Delete Edit	vlan2-0	10.4.19.236	255.255.252.0	up

At the bottom of the page, there is a copyright notice: 'Copyright © 2011 Allied Telesis Inc. All rights reserved.' and a website link: 'www.alliedtelesis.com'.

Figure 85. IPv4 Interfaces Page

The following fields are displayed:

- VLAN**— Indicates the VLAN number that has an IP interface.
- IP Address**— Indicates the IP address that the VLAN is assigned to.
- Subnet Mask**— Indicates the subnet mask of the IP address.
- Status**— Indicates the status of the link.

Adding an IPv4 Address

To assign an IPv4 address, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 84 on page 232.

2. From the Layer 3 tab, select **IPv4 Interfaces**.

A list of IPv4 interfaces is displayed. See Figure 85 on page 232.

3. Click **Add**.

The IP Address Configuration Page is displayed. See Figure 86.

The screenshot shows the IP Address Configuration page for the AT-8100S/24POE switch. The top navigation bar includes tabs for System, Switching, Security, Layer 3 (which is selected), ACLs & QoS, and Discovery & Monitoring. The sub-navigation bar shows the path: Dashboard > Layer 3 > IPv4 Interfaces > IP Address Configuration. On the right, there are **SAVE** and **LOGOUT** buttons. The main content area is titled "IP Address Configuration". It contains three input fields: "IP Address" (with a placeholder box), "Subnet Mask" (with a placeholder box), and "VLAN" (with a dropdown menu showing "Vlan1"). Below these is an "Add" button. To the right of the input fields is a "HELP" section with the following text:

IP address—Enter an IPv4 address in the following format: xxx.xxx.xxx.xxx
Subnet Mask—Enter quad-dotted decimal representation, for example, 255.255.255.0
VLAN—Select the VLAN that you would like to manage the IPv4 address on. The default VLAN is Vlan1.
 Click **Add** to save your changes to the running-configuration file.

At the bottom of the page, a copyright notice reads "Copyright © 2011 Allied Telesis Inc. All rights reserved." and the website "www.alliedtelesis.com" is listed.

Figure 86. IP Address Configuration Page

4. Enter the following fields:

- IP Address**—Enter the IP address that you want to add.
- Subnet Mask**—Enter the subnet mask of the IPv4 address in quad-dotted decimal representation, for example, 255.255.255.0.

- VLAN**— Select the VLAN ID that you want to assign the IPv4 address to.

5. Click **Add**.
6. Click **SAVE** to save your changes to the startup configuration file.

Changing an IPv4 Address

To display a list of the IPv4 interfaces, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 84 on page 232.

2. From the **Layer 3** tab, select **IPv4 Interfaces**.

A list of IPv4 interfaces is displayed. See Figure 85 on page 232.

3. From the VLANs page, click Edit next to the VLAN ID that you want to modify.

The following page is displayed. See Figure 87.

The screenshot shows the 'IP Address Configuration' page of the Allied Telesis AT-8100S/24POE web interface. The page has a header with the Allied Telesis logo, the model name 'AT-8100S/24POE', and an 'eco friendly' badge. The navigation bar includes tabs for System, Switching, Security, Layer 3 (which is selected), ACLs & QoS, and Discovery & Monitoring. The main content area shows the 'IP Address Configuration' form with fields for IP Address (192.168.2.1), Subnet Mask (255.255.255.0), and VLAN (Vlan1). Below the form is an 'Apply' button. To the right of the form is a 'HELP' box with instructions for the fields. The bottom of the page includes a copyright notice, a website link (www.alliedtelesis.com), and a 'Logout' link.

Figure 87. Edit IP Address Configuration Page

4. Change the following fields as needed:

- IP Address**— Enter the IP address that the VLAN is assigned to.
- Subnet Mask**— Enter the subnet mask of the IPv4 address.

Note

If you change the IP address that you use to access the Web interface, you lose the connection to the switch. Start a management session again by opening a web browser on your PC and entering the new IP address of the switch.

5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Deleting an IPv4 Address

To delete an IPv4 address, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 84 on page 232.

2. From the Layer 3 tab, select **IPv4 Interfaces**.

A list of IPv4 interfaces is displayed. See Figure 85 on page 232.

3. From the IPv4 Interfaces page, click Delete on the same line as the IPv4 address that you want to delete.

The selected IPv4 address is removed from the VLAN.

Displaying the IPv6 Interface

To display a list of the IPv6 interface, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 88.

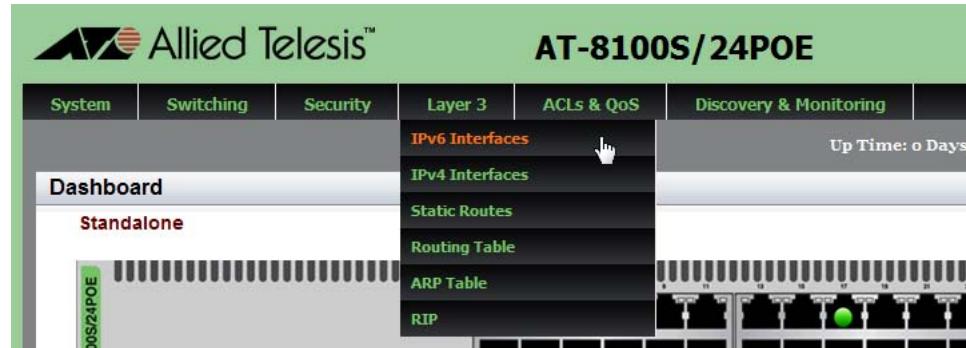


Figure 88. Layer 3 Tab

2. From the **Layer 3** tab, select **IPv6 Interface**.

The IPv6 interface is displayed if one has already been assigned. See Figure 89.

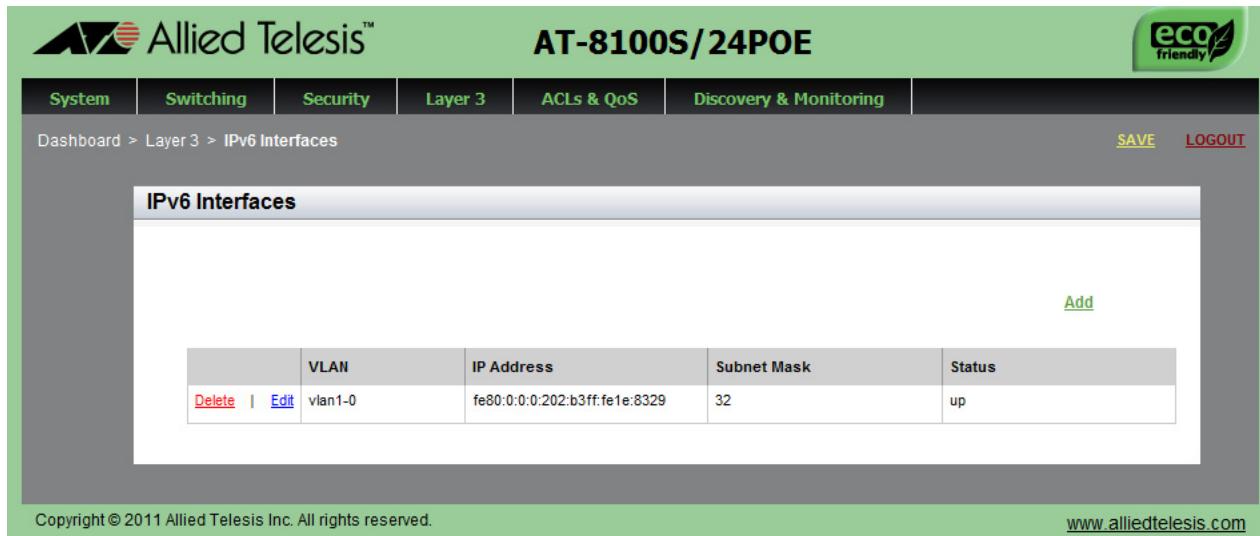


Figure 89. IPv6 Interface Page

The following fields are displayed:

- VLAN**— Indicates the VLAN number that the management IPv6 address is assigned to.
- IP Address**— Indicates the management IPv6 address.
- Subnet Mask**— Indicates the subnet mask of the management IPv6 address.
- Status**— Indicates the status of the link.

Adding an IPv6 Address

The switch supports only one IPv6 address. As a result, you can add an IPv6 address only when no IPv6 address is assigned to the switch.

To assign an IPv6 address, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 88 on page 239.

2. From the **Layer 3** tab, select **IPv6 Interface**.

The IPv6 Interface page is displayed. Ensure that no IPv6 address is displayed.

3. Click **Add**.

The IP Address Configuration Page is displayed. See Figure 90.

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 90. IPv6 Management Configuration Page

4. Select a VLAN to the IPv6 address by using the pull-down menu next to the **Interface Name** field.

You can only select a VLAN that you have configured previously. For information about how to assign a VLAN, see Chapter 11, “Setting Port-based and Tagged VLANs” on page 139.

5. Enter an IPv6 address in the **IP Address** field in the following format:

nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn:nnnn

Where n is a hexadecimal digit from 0 to F. The eight groups of digits must be separated by colons. Groups where all four digits are “0” can be omitted. Leading “0’s” in groups can also be omitted. For example, the following IPv6 addresses are equivalent:

12c4:421e:09a8:0000:0000:00a4:1c50

12c4:421e:9a8::a4:1c50

6. Enter the number of subnet mask bits in the **Subnet Mask** field.
7. Enter a IPv6 default gateway address in the **Default Gateway IP** field.

Use this field to assign the switch an IPv6 default gateway address. A default gateway is an address of an interface on a router or other Layer 3 device. It defines the first hop to reaching the remote subnets or networks where the network devices are located.

8. Click **Save**.
9. Click **SAVE** to save your changes to the startup configuration file.

Changing IPv6 Addresses

To edit the management IPv6 interface, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 88 on page 239.

2. From the **Layer 3** tab, select **IPv6 Interface**.

The IPv6 interface is displayed if one has already been assigned. See Figure 89 on page 239.

3. From the IPv6 Interface page, click Edit.

The following page is displayed. See Figure 91.

The screenshot shows the 'Edit IPv6 Management Configuration' page. The interface name is set to 'Vlan1'. The IP address is '12c4:421e:9a8:0:0:a4:'. The subnet mask is '32'. The default gateway IP field is empty. A 'HELP' panel on the right provides notes about the interface and IP address format.

Figure 91. Edit IPv6 Management Configuration Page

4. Change the following fields as needed:

- VLAN**— Select the VLAN number that the management IPv6 address is assigned to.
- IP Address**— Enter the management IPv6 address.

- Subnet Mask**— Enter the subnet mask of the management IPv6 address.
- Default Gateway IP**— Enter the default gateway IPv6 address.

5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Deleting IPv6 Addresses

To delete an IPv6 address, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 88 on page 239.

2. From the Layer 3 tab, select **IPv6 Interface**.

The IPv6 interface is displayed if any. See Figure 89 on page 239.

3. From the IPv6 Interface page, click Delete.

The management IPv6 address is removed from the switch.

Chapter 20

Access Control Lists (ACL)

This chapter provides a brief description of the ACL feature and explains how to use these features on the switch and on a port.

See the following sections:

- “Overview” on page 248
- “Creating an ACL” on page 251
- “Assigning an ACL to Ports” on page 255
- “Displaying a List of ACLs” on page 257

For information about the QoS feature, see Chapter 22, “Quality of Service (QoS)” on page 267.

For more information about the ACL feature, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Advanced Access Control Lists (ACL)
- ACL Commands

Overview

Access Control Lists (ACLs) act as filters to control the ingress packets on ports. They are commonly used to restrict the types of packets that ports accept to increase port security and create physical links dedicated to carrying specific types of traffic. For instance, you can configure ACLs to permit ports to accept only ingress packets that have a source or destination IP address.

You create an ACL first and then assign it to a port. ACLs take effect immediately when they are assigned to ports. To create an ACL, you assign filtering criteria to select a group of traffic, assign an action of dropping the traffic, forwarding the traffic to another port, or copying and sending the traffic to another port. The port filters the ingress traffic and takes an action based on the ACL that is assigned to the port.

Using the AT-8100 Web Interface, you can configure two types of ACLs:

- IPv4 ACLs
- MAC ACLs

IPv4 ACLs use IPv4 addresses as filtering criteria while MAC ACLs use only MAC addresses as filtering criteria. For IPv4 ACLs, you can specify TCP or UDP port numbers to filter the traffic. In addition, IPv4 ACLs are only compatible with IPv4 addresses. They are not compatible with IPv6 addresses.

Classifier Number Ranges

IPv4 and MAC ACLs are identified by classifier numbers. When you create an ACL, you must choose the correct classifier number based on which ACL you want to create. See the IPv4 and MAC ACL classifier number ranges displayed in Table 8.

Table 8. ACL Classifier Number Ranges

Type of ACL	Classifier Number Range
IPv4 ACLs	3000 - 3699
MAC ACLs	4000 - 4699

Filtering Criteria

ACLs identify packets using filtering criteria. The AT-8100 Web Interface offers five criteria:

- Source and destination IPv4 addresses
- Source and destination MAC addresses
- Source and destination TCP ports

- Source and destination UDP ports
- VLAN IDs

IPv4 Address and Mask

The mask of an IPv4 address is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0/24 has a mask of “24” for first the twenty-four bits of the network portion of the address. The IP address and the mask are separated by a slash (/); for example, “149.11.11.0/24.”

Actions

The action defines the response to packets that match the filtering criterion of the ACL. There are three actions for ACLs:

- Deny— A deny action instructs ports to discard the specified ingress packets.
- Permit— A permit action instructs ports to forward ingress packets that match the specified traffic flow of the ACL. By default, all ingress packets are forwarded by the ports.
- Copy to mirror— This action causes a port to copy all ingress packets that match the ACL to the destination port of the mirror port.

How Ingress Packets are Compared Against ACLs

Ports that do not have an ACL forward *all* ingress packets. Ports with one or more deny ACLs discard ingress packets that match the ACLs and forward all other traffic. A port that has one deny ACL that specifies a particular source IP address, for example, discards all ingress packets with the specified source address and forwards all other traffic. In situations where a port has more than one deny ACL, packets are discarded at the first match.

Since ports forward all ingress packets unless they have deny ACLs, permit ACLs are only necessary in situations where you want a port to forward packets that are a subset of a larger traffic flow that is blocked. For example, a port that forwards only packets having a specified destination IP address. A permit ACL specifies the packets with the intended destination IP address and a deny ACL specifies all traffic.

When ports have both permit and deny ACLs, you must add the permit ACLs first, because packets are compared against the ACLs in the order they are added to the ports. If a permit ACL is added after a deny ACL, ports are likely to discard packets specified by the permit ACL, thus causing them to block packets you want them to forward.

Guidelines

Here are the ACL guidelines:

- ❑ An ACL can have a permit, deny, or copy-to-mirror action. The permit action allows ports to forward ingress packets of the designated traffic flow while the deny action causes ports to discard packets. The copy-to-mirror action causes a port to copy all ingress packets that match the ACL to the destination port of the mirror port.
- ❑ A port can have more than one ACL.
- ❑ An ACL can be assigned to more than one port.
- ❑ ACLs filter ingress packets on ports, but they do not filter egress packets. As a result, you must apply ACLs to the ingress ports of the designated traffic flows.
- ❑ ACLs for static port trunks or LACP trunks must be assigned to the individual ports of the trunks.
- ❑ A port that has more than one ACL checks the ingress packets in the order in which the ACLs are added, and forwards or discards packets at the first match. As a result, if a port has both permit and deny ACLs, add the permit ACLs *before* the deny ACLs. Otherwise, a port is likely to discard packets you want it to forward.
- ❑ An ACL can have multiple filtering criteria. For example, an ACL filters on a source IP address and UDP port.
- ❑ Because ports, by default, forward all ingress packets, permit ACLs are only required in circumstances where you want ports to forward packets that are subsets of larger packet flows that are blocked by deny ACLs.

Creating an ACL

To create an ACL, do the following:

1. Select the **ACLs & QoS** tab.

The **ACLs & QoS** tab is displayed. See Figure 92.

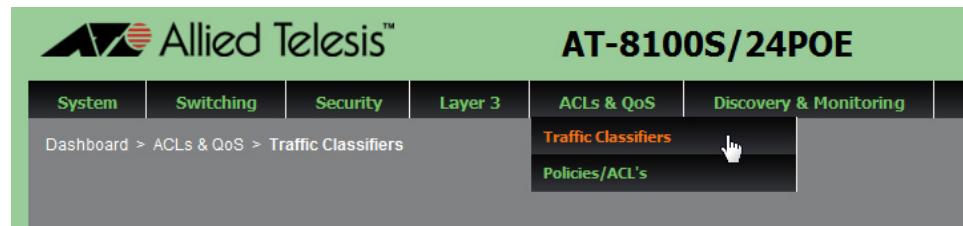


Figure 92. ACLs and QoS Tab

2. From the **ACLs & QoS** tab, select **Traffic Classifiers**.

The Traffic Classifiers page is displayed. See Figure 93.

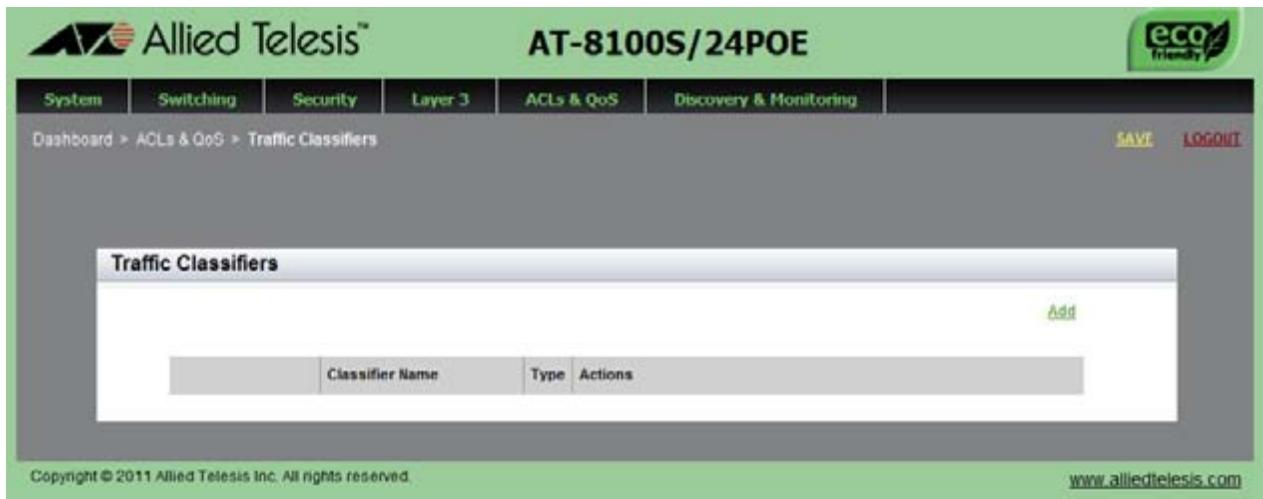


Figure 93. Traffic Classifiers Page

3. Click Add on the right above the table.

The Traffic Classification page is displayed. See Figure 94 on page 252.

The screenshot shows the 'Traffic Classification' page of the Allied Telesis AT-8100S/24POE web interface. The top navigation bar includes links for System, Switching, Security, Layer 3, ACLs & QoS, Discovery & Monitoring, and an 'ecofriendly' logo. The main content area is titled 'Traffic Classification' and contains a table for defining traffic classifiers. The table has two columns: 'Classifier #' and 'Actions'. The 'Actions' column includes icons for Deny (red hand), Permit (green checkmark), Mirror (green double arrow), Priority Queue (orange megaphone), Mark DSCP (blue bar chart), and Mark CoS (purple bar chart). Below the table is a 'Match' section with fields for Source Address, Destination Address, Source Port, Destination Port, VLAN ID, CoS, and DSCP. At the bottom of the page are 'Create Classifier' and 'Cancel' buttons. The footer includes copyright information and a website link.

Figure 94. Traffic Classification Page

4. Enter and select the following fields as needed:
 - Classifier #**— Enter a classifier number to identify an ACL. Choose a number from the following ranges:
 - IPv4 ACL:** 3000 to 3699
 - MAC ACL:** 4000 to 4699
 - Actions**— Click a radio button to select an action from the following options:
 - Deny:** Instructs ports to discard the ingress packets that match the specified filtering criteria.

Permit: Instructs ports to forward ingress packets that match the specified filtering criteria. By default, all ingress packets are forwarded by the ports.

Mirror: Instructs ports to copy all ingress packets that match the filtering criteria to the mirror port.

When you select Mirror, a text box appears below the action icons. Enter a port number (for example, port1.0.5) in the text box. The text box for Mirror to Port is displayed in Figure 95.



Figure 95. Text box for Mirror to Port

- Mirror to Port**— Enter a port number of the destination port that you want the switch to send copies of the packets that match the specified filtering criteria to.

Note

The action options of Priority Queue, Mark DSCP, and Mark CoS are for the Quality of Service (QoS) feature. For information about creating a QoS policy, see “Creating a QoS Policy” on page 271.

Match:

- Source Address**— Enter a source address to match ingress packets. Enter one of the following:

The keyword “any:” Matches all packets on the source address.

IPv4 Address and mask: Enter an IPv4 source address followed by an slash (/) and a mask if you are creating an IPv4 ACL.

MAC Address and mask: Enter an MAC source address followed by an slash (/) and a mask if you are creating a MAC ACL.

- Destination Address**— Enter a destination address to match ingress packets. Enter one of the following:

The keyword “any:” Matches all packets on the destination address.

IPv4 Address and mask: Enter an IPv4 source address followed by an slash (/) and a mask if you are creating an IPv4 ACL.

MAC Address and mask: Enter an MAC source address followed by an slash (/) and a mask if you are creating a MAC ACL.

Note

The Source Port and Destination Port fields are applicable only for IPv4 ACLs.

- Source Port**— Select TCP or UDP from the pull-down menu and enter a source port number as needed. This field is optional.
- Destination Port**— Select TCP or UDP from the pull-down menu and enter a source port number as needed. This field is optional.
- VLAN ID**— Enter a VLAN ID. Use this field if you want the ACL to filter tagged packets. This field is optional.

Note

The matching criteria of **CoS** and **DSCP** are for the Quality of Service (QoS) feature. For information about creating a QoS, see “Creating a QoS Policy” on page 271.

5. Click **Create Classifier**.
6. Click **SAVE** to save your changes to the startup configuration file.

Assigning an ACL to Ports

Before assigning ACLs to ports, ACLs must be available on the switch. To create an ACL, see “Creating an ACL” on page 251.

To assign an ACL to ports, do the following:

1. Select the **ACLs &QoS** tab.

The **ACLs & QoS** tab is displayed. See Figure 92 on page 251.

2. From the **ACLs & QoS** tab, select **Policies/ACLs**.

The Policies/ACLs page is displayed. See Figure 96.

	Classifier Name	Type	Interface
Delete	3001	ACL	
Delete	3002	ACL	
Delete	4001	ACL	

Figure 96. Policies/ACLs Page

3. Click Add on the right above the table.

The Traffic Classifiers page is displayed. See Figure 97 on page 256.

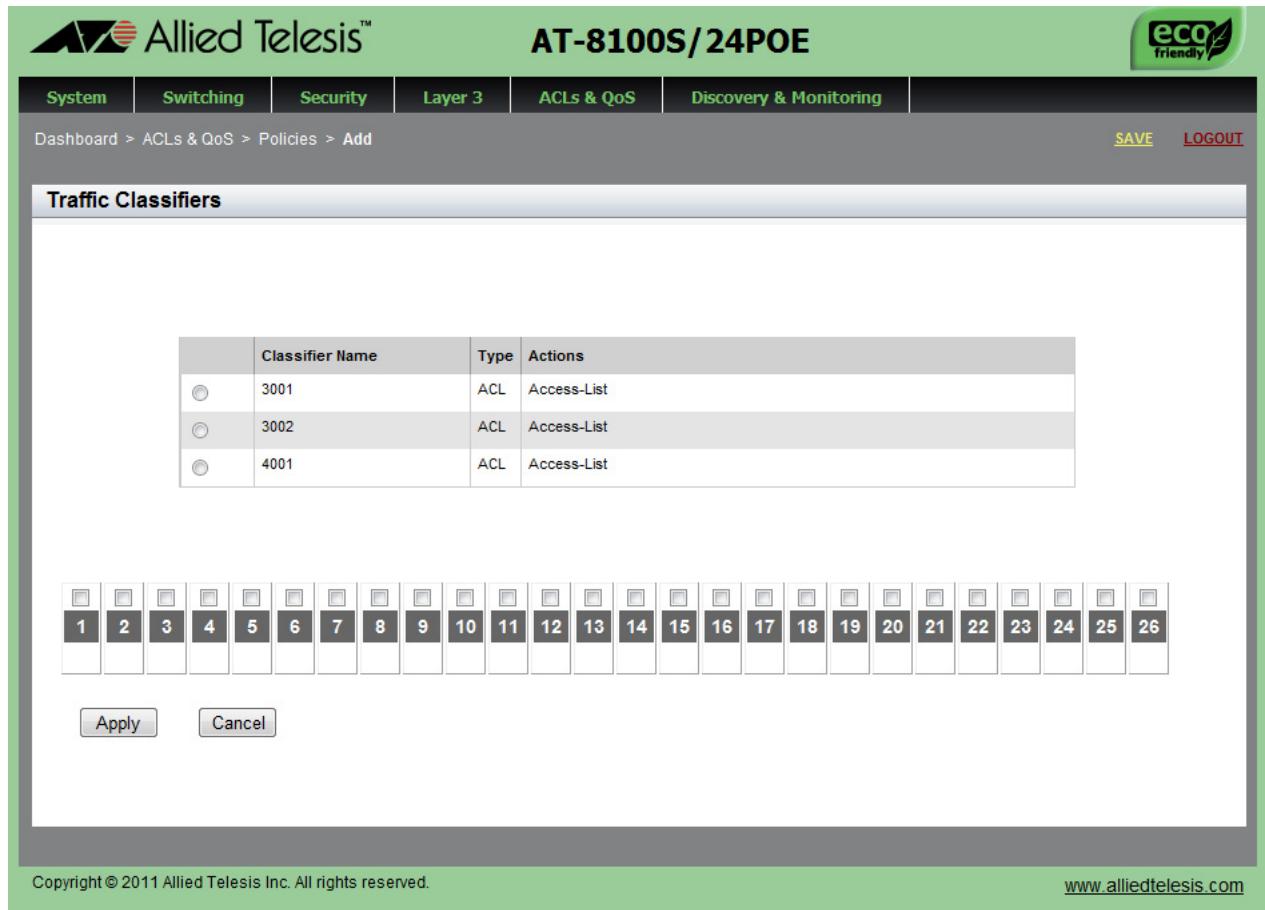


Figure 97. Traffic Classifiers Page

4. Click a radio button to select an ACL.
5. Check one or multiple checkboxes to select ports to apply the ACL.
6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Displaying a List of ACLs

To display a list of ACLs, do the following:

1. Select the **ACLs &QoS** tab.

The **ACLs & QoS** tab is displayed. See Figure 92 on page 251.

2. From the **ACLs & QoS** tab, select **Traffic Classifiers**.

The Traffic Classifiers page is displayed. See Figure 98.

	Classifier Name	Type	Actions
Delete View	3001	ACL	PERMIT
Delete View	3002	ACL	COPY-TO-MIRROR
Delete View	4001	ACL	DENY

Figure 98. Traffic Classifiers Page

3. The following fields are displayed:

- Classifier Number**— Indicates an ACL or QoS classifier number.
- Type**— Indicates either ACL or QoS.
- Actions**— Lists actions specified to the classifier.

Note

This list includes QoS policies as well as ACLs.

Chapter 21

Setting Static Routes

To make remote networks communicate, you must add static routes or dynamic routes, or both to the routing table. Static routes are configured manually to add routing information to the routing table. This chapter provides information about static routes.

The procedures in this chapter describe how to display a list of static routes on the switch, and how to add and delete a static route. See the following sections:

- “Displaying Static Routes” on page 260
- “Adding a Static Route” on page 262
- “Deleting a Static Route” on page 264
- “Displaying the Routing Table” on page 265

For more information about static routes, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Internet Protocol Version 4 Packet Routing
- IPv4 Routing Commands

Displaying Static Routes

To display the static routes, do the following:

1. Select the Layer 3 tab.

The Layer 3 tab is displayed. See Figure 99.

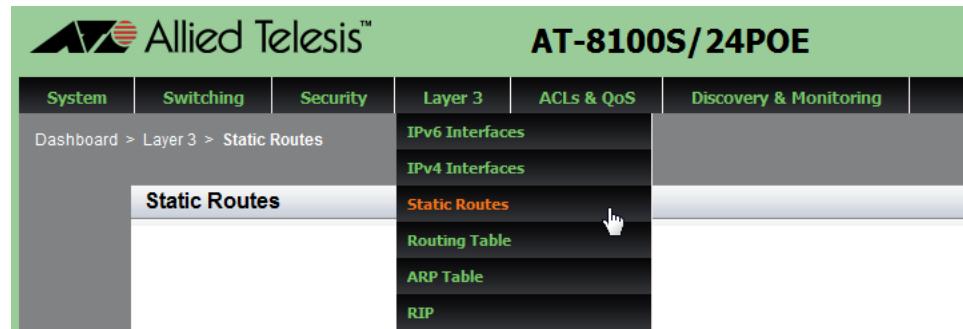


Figure 99. Layer 3 Tab

2. From the Layer 3 tab, select **Static Routes**.

A list of static routes is displayed. See Figure 100.

	Network Address	Network Mask	Next Hop	AD
Delete	0.0.0.0	0.0.0.0	192.168.100.1	1
Delete	192.168.100.0	255.255.255.0	192.168.100.234	1

Figure 100. Static Routes Page

The following fields are displayed:

- Network Address**— Indicates the IP address of the destination network. The IP address for a default route is 0.0.0.0.

- Network Mask**— Indicates the subnet mask of the destination network.
- Next Hop**— Indicates the IP address of the next hop to the route.
- AD**— Indicates the value of the administrative distance specified to the route.

Adding a Static Route

To add a static route, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 99 on page 260.

2. From the Layer 3 tab, select **Static Routes**.

A list of static routes is displayed. See Figure 100 on page 260.

3. Click **Add**.

The Add Static Route Page is displayed. See Figure 101.

The screenshot shows the 'Enter Static Route' page of the Allied Telesis AT-8100S/24POE web interface. The page has the following fields:

- Network Address:** 0.0.0.0
- Network Mask:** 0.0.0.0
- Next Hop:** 10.4.16.1
- AD(1-255):** 1 (Optional)

Below the fields is a 'Help' box with the following text:

HELP

Network Address—Enter the IPv4 address of the destination network. To enter the default route, enter: 0.0.0.0

Network Mask—Enter the subnet mask of the destination network, for example, 255.255.255.0. To enter the subnet mask of the default route, enter: 0.0.0.0

Next Hop—Enter the IPv4 address of the next hop to the route.

AD (1-255)—Enter the value of the administrative distance specified to

At the bottom of the page, there is a 'SAVE' button and a 'Logout' link.

Figure 101. Add Static ARP Page

4. Enter the destination network address in the **Network Address** field.
5. Enter the subnet mask of the destination network in the **Network Mask** field.
6. Enter the IP address of the next hop in the **Next Hop** field.

7. Enter the value of the metric for the route in the **AD** field. The range is 1 to 255.

The field is optional. The default is 1.

8. Click **Add**.
9. Click **SAVE**.

Deleting a Static Route

To delete a static route entry, do the following:

1. Select the Layer 3 tab.

The Layer 3 tab is displayed. See Figure 99 on page 260.

2. From the Layer 3 tab, select **Static Routes**.

A list of static routes is displayed. See Figure 100 on page 260.

3. Click Delete next to the network address that you want to delete.

Displaying the Routing Table

The routing table includes static routes and dynamic routes. The switch decides which route is the best based on the routing table.

To display the routing table, do the following:

1. Select the Layer 3 tab.

The Layer 3 tab is displayed. See Figure 99.



Figure 102. Layer 3 Tab

2. From the Layer 3 tab, select **Routing Table**.

A list of routes is displayed. See Figure 103.

Destination	Network Mask	NextHop	Interface	Protocol	AD/Metric
0.0.0.0	0.0.0.0	10.4.16.1	vlan2	Static	100/0
10.4.16.0	255.255.252.0	N/A	vlan2	Connected	N/A

Figure 103. Routing Table Page

The following fields are displayed:

- Destination**— Indicates the destination network address.
- Network Mask**— Indicates the subnet mask of the destination network address.
- Nexthop**— Indicates the IP address of the next hop to the route.
- Interface**— Indicates the VLAN ID of the interface.
- Protocol**— Indicates how this route is established.

“Static” indicates that the route was added statically; “RIP” indicates that the route was added dynamically using the RIP protocol; “Connected” indicates that the route is connected directly.

- AD/Metric**— Indicates the value of the administrative distance specified to the route, and the number of routing devices a packet must travel through to reach the destination.

Chapter 22

Quality of Service (QoS)

This chapter provides a brief description of the QoS feature and explains how to use the feature on the switch and on a port.

See the following sections:

- “Overview” on page 268
- “Creating a QoS Policy” on page 271
- “Assigning a QoS Policy to Ports” on page 276
- “Displaying a List of QoS Policies” on page 278

For information about the ACL feature, see Chapter 20, “Access Control Lists (ACL)” on page 247.

For more information about the QoS feature, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Quality of Service (QoS)
- Quality of Service (QoS) Commands

Overview

Quality of Service (QoS) is a feature that classifies and prioritizes traffic to guarantee a certain level of performance in converged networks, which run voice and video services on data networks. Without QoS, all traffic types are equally likely to be dropped when congestion occurs. QoS can give certain traffic types preferential treatment. For example, QoS is used to provide the users of IP phones the same quality of voice transmission as conventional telephone service provides. With QoS, you can ensure that voice packets have a higher priority throughout the network.

To give the different forwarding treatment to traffic, QoS assigns a priority class to packets upon entry into the network. Then, switches and routers along the path use the class information to select a certain behavior for the packet and provide appropriate QoS treatment.

Class Information

In the Layer 3 IP packet, the class information is carried in the Differentiated Services Code Point (DSCP) field. The class information can also be carried as a Class of Service (CoS) value in the Layer 2 frame. Layer 2 Inter-Switch Link (ISL) frame headers have a User field that carries a class of service (CoS) value; Layer 2 802.1Q frame headers have a Tag Control Information field that carries the CoS value.

You can use DSCP and CoS values as filtering criteria to classify incoming packets. You also can configure QoS to assign a new value to the DSCP and CoS to the packets that match the specified filtering criteria.

Priority Queue

Each egress port has eight egress queues allocated. By default, all queues on all ports are serviced in strict priority order. This means that the highest numbered priority queue, queue 7, is emptied first. When queue 7 is completely empty, the next highest priority queue, queue 6, is processed. This process is continued until you reach queue 0. For a strict priority queue to be processed, all higher priority queues must be empty.

You can configure QoS to set the packets that match the specified filtering criteria to an egress queue on a port.

Classifier Number Ranges

QoS policies are identified by classifier numbers. When you create a QoS policy, you must choose the correct classifier number based on whether you specify an IP address or MAC address as a filtering criterion. See the classifier number ranges for QoS policies in Table 9 on page 269.

Table 9. Classifier Number Ranges for QoS

Filtering Criterion	Classifier Number Range
Specifying an IPv4 address	3000 - 3699
Specifying an MAC address	4000 - 4699
Specifying no address	3000 - 3699 and 4000 - 4699

Filtering Criteria

QoS policies identify packets using filtering criteria. The AT-8100 Web Interface offers seven criteria:

- Source and destination IP addresses
- Source and destination MAC addresses
- Source and destination TCP ports
- Source and destination UDP ports
- VLAN IDs
- CoS value
- DSCP value

Actions

The action defines the response to packets that match the filtering criteria of a QoS policy. There are three actions that you can choose from using the AT-8100 Web Interface:

- Priority Queue— This action causes a port to place all ingress packets that match the filtering criteria to the specified priority queue.
- Mark DSCP— This action causes a port to change the DSCP value of all ingress packets that match the filtering criteria with the specified DSCP value.
- Mark CoS— This action causes a port to change the CoS value of all ingress packets that match the filtering criteria with the specified CoS value.

How Ingress Packets are Selected with Filtering Criteria

A QoS policy can have more than one filtering criterion. A QoS policy that has one filtering criterion that specifies a particular source IP address, for example, selects only packets with the specified source address and applies the specified action. A QoS policy that has two filtering criteria that specified a particular VLAN ID and DSCP value, for example, selects only packets that matches the specified VLAN ID and CoS value.

Guidelines

Here are the QoS guidelines:

- A QoS can have a “Priority Queue,” “Mark DSCP,” or “Mark CoS” action. The priority queue action allows a port to place ingress packets that match the filtering criteria to the specified priority queue. The Mark

DSCP action causes a port to change the DSCP value of all ingress packets that match the filtering criteria with the specified DSCP value. The mark CoS action causes a port to change the CoS value of all ingress packets that match the filtering criteria with the specified Cos value.

- A port can have only one QoS policy.
- A QoS policy can be assigned to more than one port.
- QoS classifies ingress packets, but does not process egress packets. As a result, you must apply QoS policies to the ingress ports of the designated traffic flows.
- QoS policies for static port trunks or LACP trunks must be assigned to the individual ports of the trunks.
- A QoS policy can have multiple filtering criteria. For example, a QoS may classify traffic based on a source IP address, a VLAN ID, and a DSCP value.
- A QoS policy that has more than one filtering criterion selects traffic that matches all specified filtering criteria.

Creating a QoS Policy

To create an QoS, do the following:

1. Select the **ACLs &QoS** tab.

The **ACLs & QoS** tab is displayed. See Figure 104.

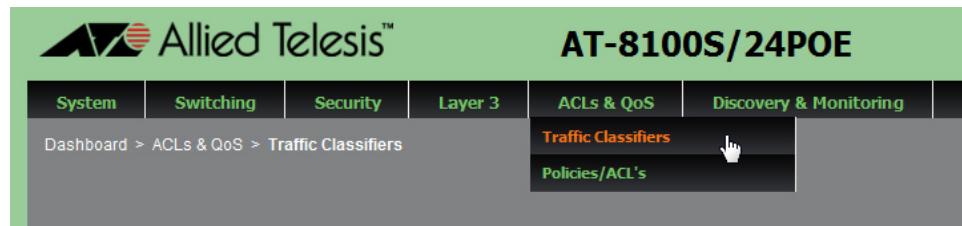


Figure 104. ACLs and QoS Tab

2. From the **ACLs & QoS** tab, select **Traffic Classifiers**.

The Traffic Classifiers page is displayed. See Figure 105.



Figure 105. Traffic Classifiers Page

3. Click Add on the right above the table.

The Traffic Classification page is displayed. See Figure 106 on page 272.

AT-8100S/24POE

System | Switching | Security | Layer 3 | ACLs & QoS | Discovery & Monitoring | **Layer 3**

Dashboard > ACLs & QoS > Traffic Classifiers > Add Traffic Classifier

Traffic Classification

Classifier #	Actions
IPv4: 3000 - 3699 MAC: 4000 - 4699	Deny <input type="radio"/> Permit <input type="radio"/> Mirror <input type="radio"/> Priority Queue <input type="radio"/> Mark DSCP <input type="radio"/> Mark CoS <input type="radio"/>

Match

Source Address	Destination Address	Source Port	Destination Port
None <input type="button" value=""/>			
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
VLAN ID	CoS	DSCP	
<input type="text"/>	None <input type="button" value=""/>	None <input type="button" value=""/>	

Create Classifier **Cancel**

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 106. Traffic Classification Page

- Enter and select the following fields as needed:
 - Classifier #**— Enter a classifier number to identify a QoS policy. Choose a classifier number according to the following conditions:
 - When specifying an IPv4 address as a filtering criterion:** Choose from 3000 to 3699.
 - When specifying a MAC Address as a filtering criterion:** Choose from 4000 to 4699.
 - When not specifying an address as a filtering criterion:** Choose from 3000 to 3699 or from 4000 to 4699.

Actions— Click a radio button to select an action from the following options:

Priority Queue: Instructs ports to place all ingress packets that match the filtering criteria into a specified priority queue.

When you select Priority Queue, a text box appears below the action icons as shown in Figure 107. Enter a priority queue number. Choose from 0 to 7.

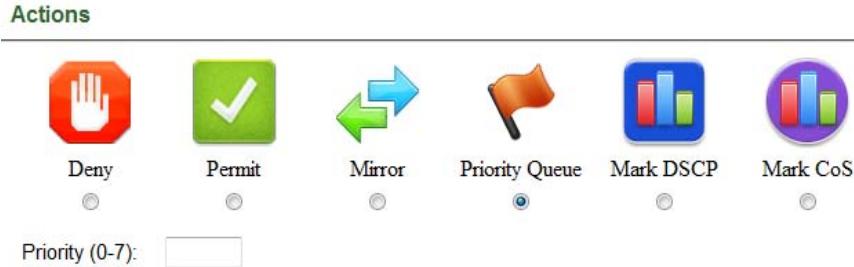


Figure 107. Text box for Priority Queue

Mark DSCP: Instructs ports to set the DSCP value in all ingress packets that match the filtering criteria with specified DSCP value.

When you select Mark DSCP, a text box appears below the action icons as shown in Figure 108. Enter a DSCP value. Choose from 0 to 63.

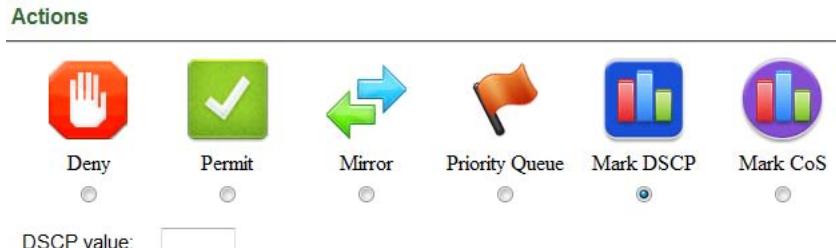


Figure 108. Text box for DSCP

Mark CoS: Instructs ports to set the CoS value in all ingress packets that match the filtering criteria with a specified CoS value.

When you select Mark CoS, a text box appears below the action icons shown in Figure 109 on page 274. Enter a CoS value. Choose from 0 to 7.

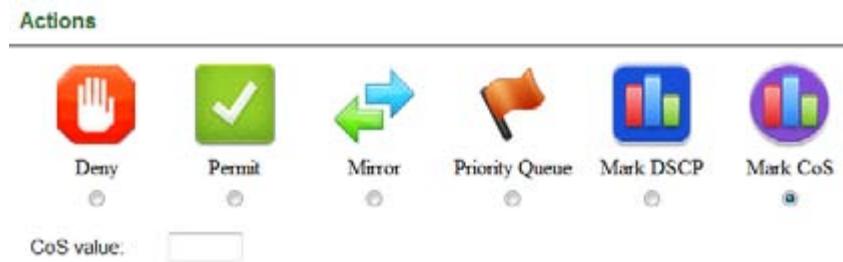


Figure 109. Text box for CoS

Note

The action options of Deny, Permit, and Mirror are for the Access Control List (ACL) feature. For information about creating an ACL, see “Creating an ACL” on page 251.

Match

The following parameters are under the “Match” heading on the Traffic Classification Page.

Note

You can specify one or more match criteria to create a QoS policy.

- Source Address**— Specify a source address to match ingress packets as needed. Enter one of the following:

The keyword “any:” Matches all packets on the source address.

IPv4 Address and mask: Enter an IPv4 source address followed by an slash (/) and a mask if you are creating an IPv4 ACL.

MAC Address and mask: Enter an MAC source address followed by an slash (/) and a mask if you are creating a MAC ACL.

- Destination Address**— Specify a destination address to match ingress packets as needed. Enter one of the following:

The keyword “any:” Matches all packets on the destination address.

IPv4 Address and mask: Enter an IPv4 source address followed by an slash (/) and a mask if you are creating an IPv4 ACL.

MAC Address and mask: Enter an MAC source address followed by an slash (/) and a mask if you are creating a MAC ACL.

- Source Port**— Select TCP or UDP from the pull-down menu and enter a source port number as needed.
- Destination Port**— Select TCP or UDP from the pull-down menu and enter a source port number as needed.
- VLAN ID**— Enter a VLAN ID. Use this field if you want the ACL to filter tagged packets.
- CoS**— Select a CoS value from the pull-down menu as needed. Choose from 0 to 7.
- DSCP**— Select a DSCP value from the pull-down menu as needed. Choose from 0 to 63.

5. Click **Create Classifier**.
6. Click **SAVE** to save your changes to the startup configuration file.

Assigning a QoS Policy to Ports

Before assigning QoS policies to ports, QoS policies must be available on the switch. For how to create a QoS policy, see “Creating a QoS Policy” on page 271.

To assign a QoS policy to ports, do the following:

1. Select the **ACLs & QoS** tab.

The **ACLs & QoS** tab is displayed. See Figure 104 on page 271.

2. From the **ACLs & QoS** tab, select **Policies/ACLs**.

The Policies/ACLs page is displayed. See Figure 110.

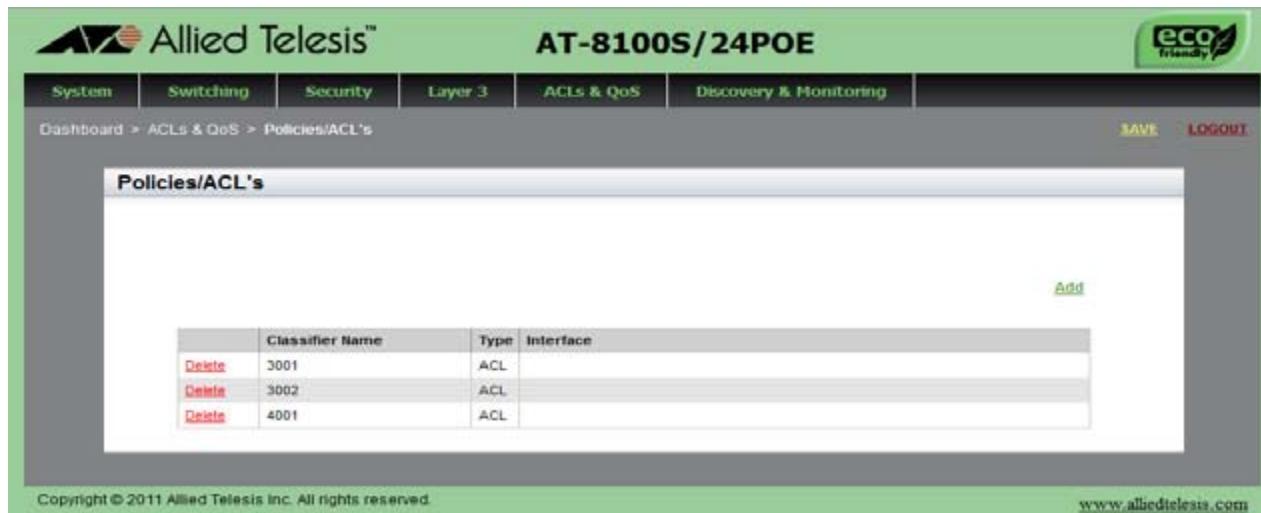


Figure 110. Policies/ACLs Page

3. Click Add on the right above the table.

The Traffic Classifiers page is displayed. See Figure 111 on page 277.

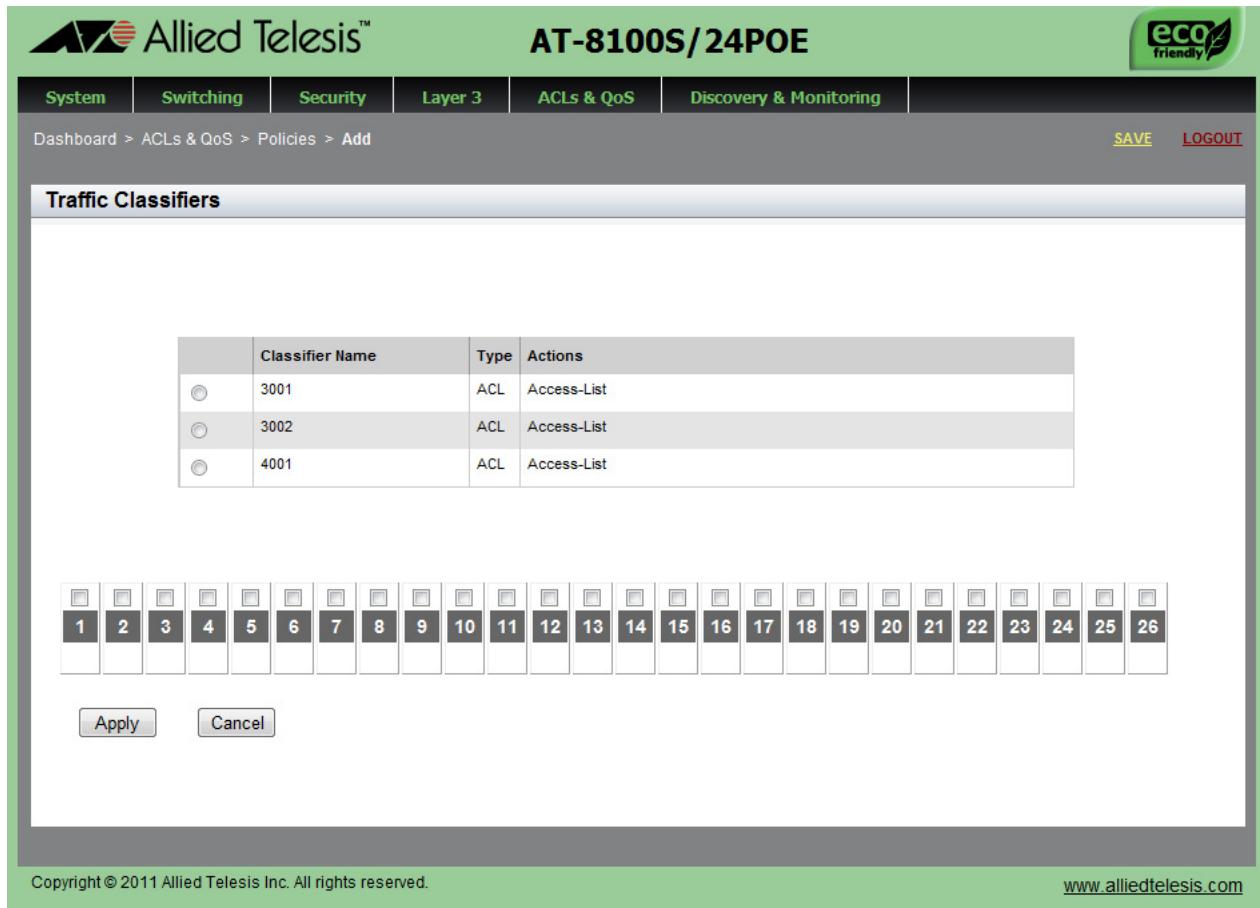


Figure 111. Traffic Classifier Page

4. Click a radio button to select a QoS policy.
5. Check one or multiple checkboxes to select ports to apply the QoS policy.
6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Displaying a List of QoS Policies

To display a list of ACLs, do the following:

1. Select the **ACLs & QoS** tab.

The **ACLs & QoS** tab is displayed. See Figure 104 on page 271.

2. From the **ACLs & QoS** tab, select **Traffic Classifiers**.

The Traffic Classifiers page is displayed. See Figure 112.

	Classifier Name	Type	Actions
Delete View	3001	ACL	PERMIT
Delete View	3002	ACL	COPY-TO-MIRROR
Delete View	4001	ACL	DENY

Figure 112. Traffic Classifiers Page

3. The following fields are displayed:

- Classifier Number**— Indicates an ACL or QoS classifier number.
- Type**— Indicates either ACL or QoS.
- Actions**— Lists actions specified to the classifier.

Note

This list includes ACLs as well as QoS policies.

Chapter 23

Setting Dynamic Routes Using RIP

The chapter provides a brief description of the RIP feature and explains how to display the RIP settings, enable RIP on a VLAN interface, change the RIP settings, delete a VLAN interface, and display RIP statistics. See the following sections:

- “Overview” on page 280
- “Displaying the RIP Configuration” on page 281
- “Enabling RIP on a VLAN Interface” on page 283
- “Changing the RIP Settings” on page 286
- “Removing a VLAN Interface from the RIP Configuration” on page 287
- “Displaying RIP Statistics” on page 288

For more information about RIP, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Routing Information Protocol (RIP)
- Routing Information Protocol (RIP) Commands

Overview

To make remote networks communicate, you must add either static routes, dynamic routes, or both. The AlliedWare Plus™ Management Software supports RIP as the routing protocol to add dynamic routes. By enabling RIP, the switch can learn about remote networks and add the routing information to its routing table dynamically. For information about static routes, refer to Chapter 21, “Setting Static Routes” on page 259.

Enabling RIP

Here are guidelines for enabling RIP:

- A VLAN interface must have an IP address assigned before RIP is enabled on the interface.
- To make a switch access to remote networks, you must configure RIP on a VLAN interface or network that is connected to another Layer 3 device and remote networks that you want the switch to access to.
- Authentication is supported only in RIP Version 2.

Note

To display the routing table that includes both dynamic routes and static routes, see “Displaying the Routing Table” on page 265.

Displaying the RIP Configuration

To check how the RIP is configured on the switch, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 113.

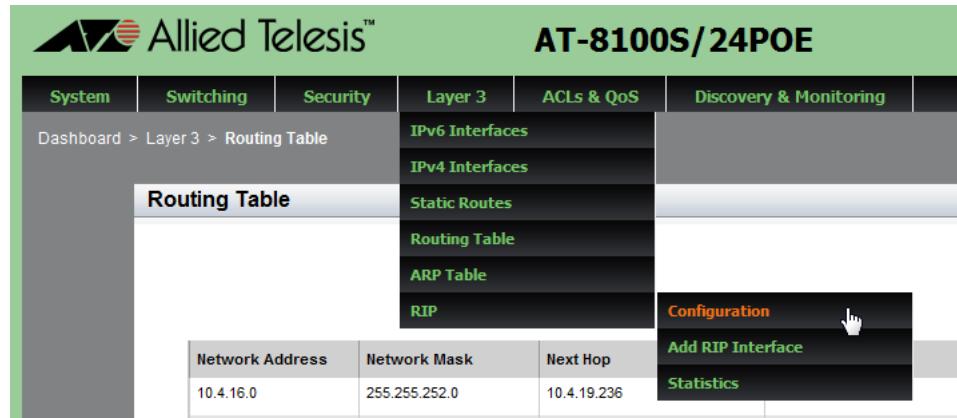


Figure 113. Layer 3 Tab

2. From the Layer 3 tab, select or move the cursor over RIP and select **Configuration**.

The RIP configuration page is displayed. See Figure 114.

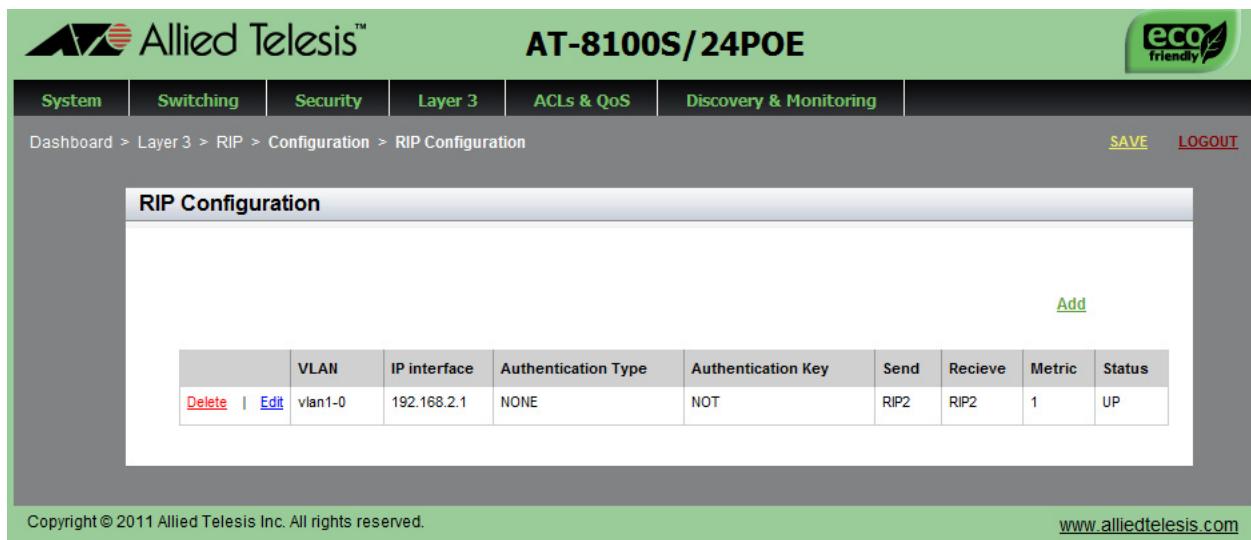


Figure 114. RIP Configuration Page

The following fields are displayed:

- VLAN**— Indicates the ID number of the VLAN. This VLAN interface receives and sends RIP packets and the network that the VLAN belongs to is advertised through RIP.
- IP Interface**— Indicates the IP address that the VLAN interface is assigned to.
- Authentication Type**— Indicates the ID number of the VLAN where the host is a member.
- Authentication Key**— Indicates the port number where the host is connected.
- Send**— Indicates the RIP version number of the packets that the VLAN interface is specified to send.
- Receive**— Indicates the RIP version number of the packets that the VLAN interface is specified to receive.
- Metric**— Indicates the number of routing devices that a packet must travel to reach the destination.
- Status**— Indicates the status of the VLAN interface.

Enabling RIP on a VLAN Interface

To enable RIP and connect remote networks dynamically, you must enable RIP on VLAN interfaces. When RIP is enabled on a VLAN interface, the VLAN interface sends and receives RIP packets, and the network where the VLAN belongs is advertised through RIP.

To enable RIP on a VLAN interface, you must add the VLAN to the RIP routing process by performing the following procedure:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 115.

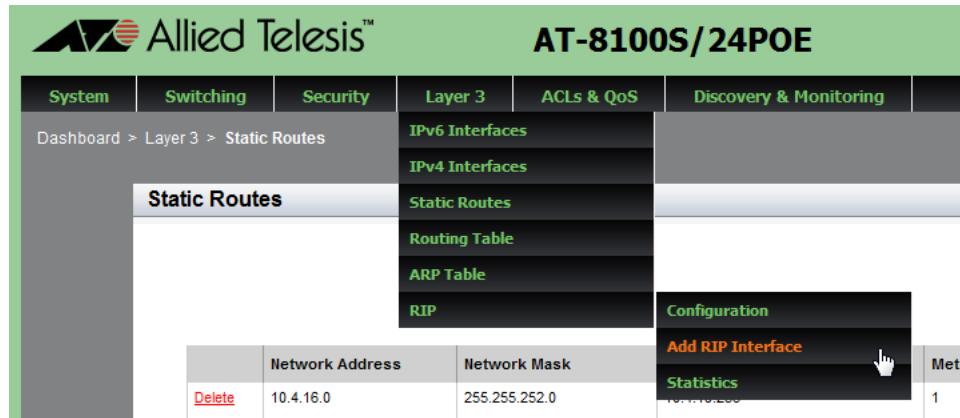


Figure 115. Layer 3 Tab

2. From the Layer 3 tab, select or move the cursor over RIP and select **Add RIP Interface**.

The RIP Interface page is displayed. See Figure 116 on page 284.

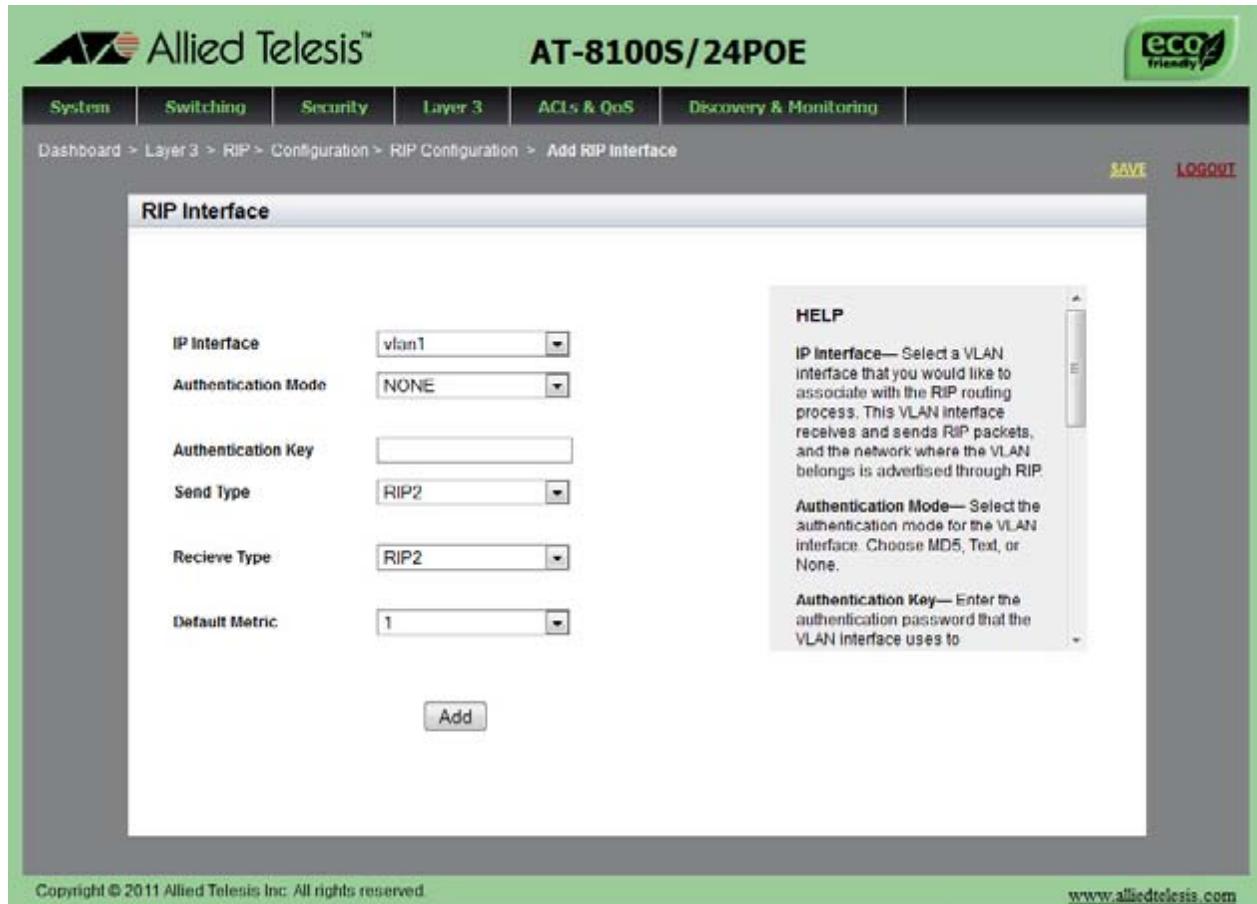


Figure 116. RIP Interface Page

3. Specify the following fields as needed:

- VLAN Interface**— Select the VLAN interface to associate with the RIP routing process. This VLAN interface receives and sends RIP packets and the network where the VLAN belongs is advertised through RIP.
- Authentication Mode**— Select the authentication mode for the VLAN interface. Choose MD5, Text, or None.
- Authentication Key**— Enter the authentication password that the VLAN interface uses to authenticate the RIP packets. The authentication password can be up to sixteen alphanumeric characters. It is case-sensitive and can include spaces.
- Send Type**— Select the RIP version of packets that the VLAN interface sends. Choose RIP1 or RIP2.
- Receive Type**— Select the RIP version of packets that the VLAN interface receives. Choose RIP1, RIP2, or Both.
- Default Metric**— Select the Default Metric value. Choose a number from 1 to 16.

4. Click **Add**.
5. Click **SAVE** to save your changes to the startup configuration file.

Note

There is another way to go to the RIP Interface page to enable RIP on a VLAN interface. Go to the RIP Configuration page from the RIP Configuration page shown in Figure 114 on page 281 and click **Add**. To go to the RIP Configuration page, see the procedure in “Displaying the RIP Configuration” on page 281.

Changing the RIP Settings

To change the RIP settings of the VLAN interface, perform the following:

1. Select the Layer 3 tab.

The Layer 3 tab is displayed. See Figure 113 on page 281.

2. From the Layer 3 tab, select or move the cursor over **RIP** and select **Configuration**.

The RIP Configuration page is displayed. See Figure 114 on page 281.

3. Click **Edit** next to the VLAN that you want to edit.

The RIP Interface page is displayed. See Figure 116 on page 284.

Removing a VLAN Interface from the RIP Configuration

To remove a VLAN interface from the RIP configuration, do the following:

1. Select the Layer 3 tab.

The Layer 3 tab is displayed. See Figure 113 on page 281.

2. From the Layer 3 tab, select **RIP** or move the cursor over **RIP** and select **Configuration**.

The RIP configuration page is displayed. See Figure 114 on page 281.

3. Click **Delete** next to the VLAN that you want to remove.

Displaying RIP Statistics

To display counters for RIP packets on the switch, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 117.

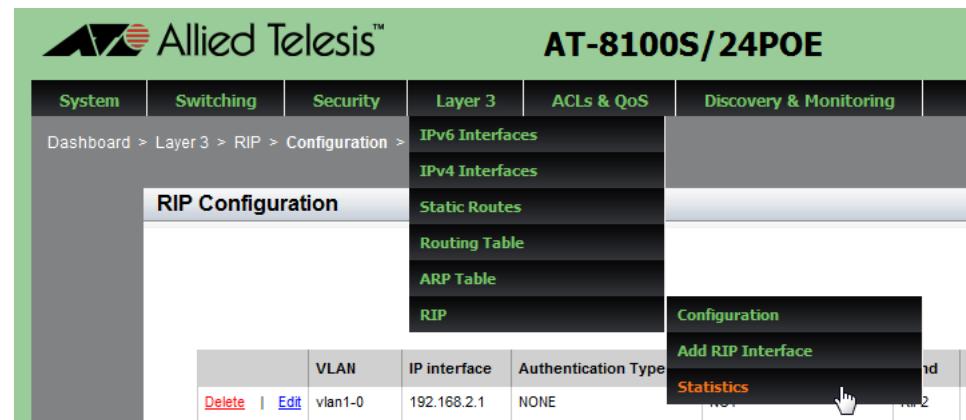


Figure 117. Layer 3 Tab

2. From the Layer 3 tab, select **RIP** or move the cursor over **RIP** and select **Statistics**.

The RIP statistics page is displayed. See Figure 118.

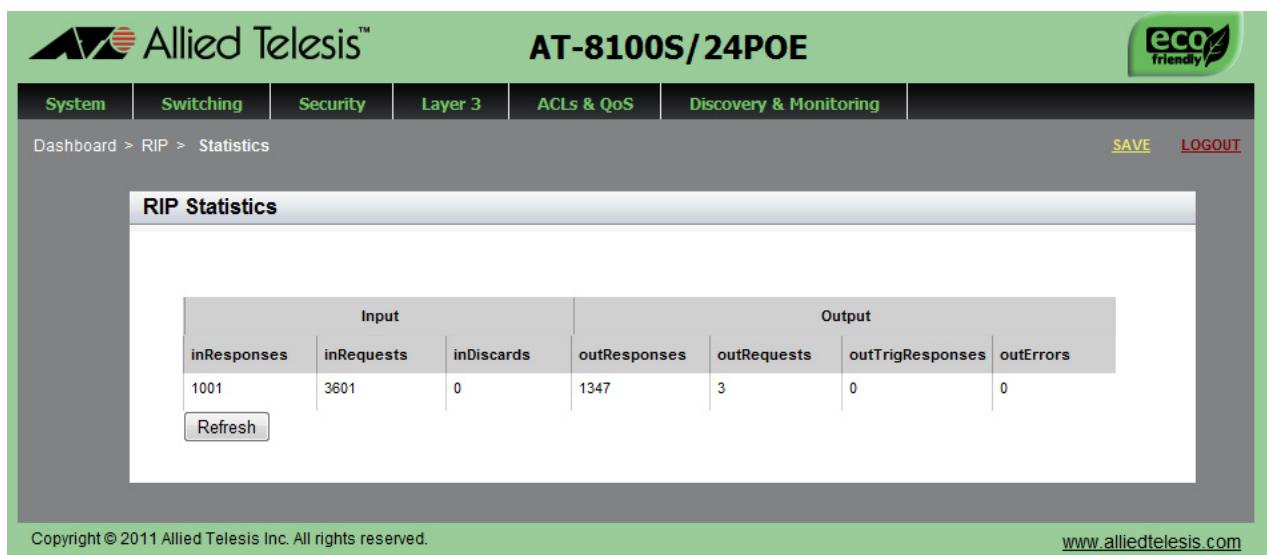


Figure 118. RIP Configuration Page

The following fields are displayed:

- Input**— Indicates that the counters displayed under this column are for incoming RIP packets.
- inResponses**— Indicates the number of response packets received.
- inRequests**— Indicates the number of request packets received.
- inDiscards**— Indicates the number of packets discarded. Packets may be discarded due to authentication failure, packet received when receive is disabled, or mismatched sequence number of a triggered acknowledgement.
- Output**— Indicates that the counters under this column are for outgoing RIP packets.
- outResponses**— Indicates the number of response packets transmitted.
- outRequests**— Indicates the number of request packets transmitted.
- outTrigResponses**— Indicates the number of triggered response packets transmitted.
- outErrors**— Indicates the number of packets with errors.

Reloading RIP Statistics

RIP statistics are constantly counting up so that the data that has been displayed in the RIP Statistics pages is not the most recent. To display the latest data possible, click on the **Refresh** button on the RIP Statistics page.

Figure 119 shows the Refresh button on the RIP Statistics page.

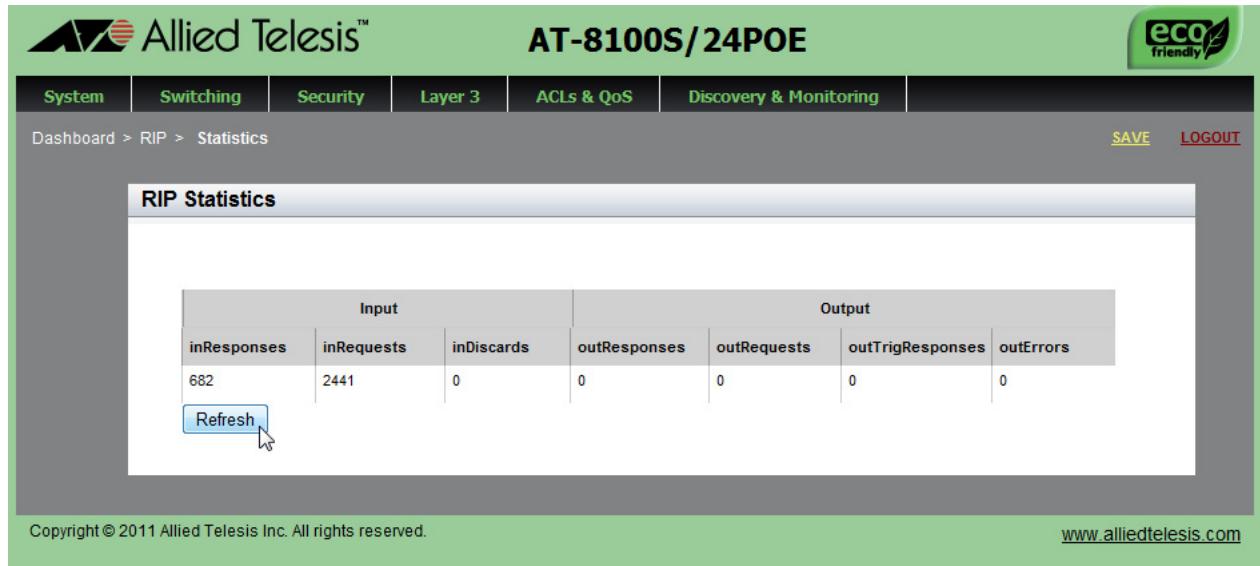


Figure 119. RIP Statistics Page with the Refresh Button

Chapter 24

Managing the ARP Table

The procedures in this chapter describe how to display the ARP table that resides on the switch, how to add static ARP entries to the table, and how to delete static ARP entries.

See the following sections:

- “Overview” on page 292
- “Displaying the ARP Table” on page 293
- “Adding a Static ARP Entry” on page 295
- “Deleting ARP Entries” on page 297

For more information about ARP, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- Address Resolution Protocol (ARP)
- Address Resolution Protocol (ARP) Commands

Overview

The Address Resolution Protocol (ARP) is used to associate an IPv4 address with a MAC address used by network nodes including the AT-8100 switches. ARP gathers information about mapping between an IPv4 address and a MAC address and stores them in the ARP table. When the node receives a packet from the Network layer, then the node encapsulates the packet into a frame. The node looks up the ARP cache to find out the MAC address of the destination node. The ARP table is populated dynamically; however, the AT-8100 switches allow you to add static ARP entries, which are entered manually.

ARP Table Management Guidelines

See the following list for guidelines about managing the ARP table on the AT-8100 switches:

- The dynamic ARP entries are time-stamped and set to time out in 300 seconds.
- The dynamic ARP entries are not deleted individually and must be deleted altogether if you want to delete them before they time out.
- The switch supports up to 512 static ARP entries.
- The static ARP entries never expire. You must remove them manually as needed. You can delete them individually.

Displaying the ARP Table

To display the ARP table, do the following:

1. Select the Layer 3 tab.

The Layer 3 tab is displayed. See Figure 120.

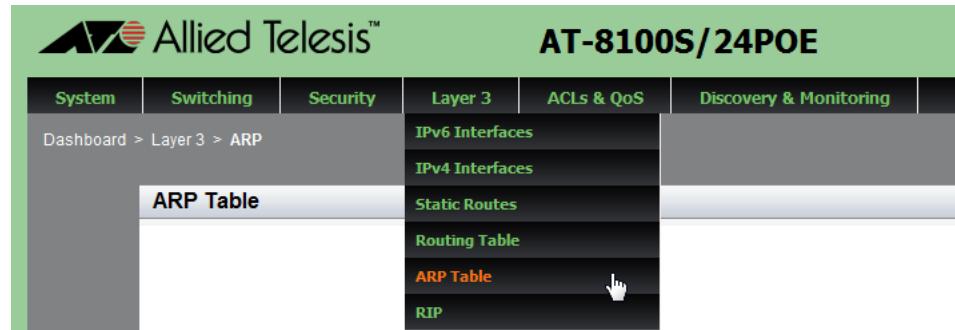


Figure 120. Switching Tab

2. From the Layer 3 tab, select **ARP Table**.

The ARP table is displayed. See Figure 121.

	IP Address	MAC Address	VLAN	Port	Type
Delete	10.4.16.1	0000.cd37.083f	vlan1-0	port1.0.3	Dynamic
Delete	10.4.16.54	5c26.0a04.9nh9	vlan1-0	port1.0.3	Dynamic
Delete	10.4.16.56	5c26.0a2d.2e0e	vlan1-0	port1.0.3	Dynamic
Delete	10.4.16.57	5094.6ba7.3c3c	vlan1-0	port1.0.3	Dynamic
Delete	10.4.16.62	5894.6b0c.ddfc	vlan1-0	port1.0.3	Dynamic
Delete	10.4.16.64	842b.2bab.e933	vlan1-0	port1.0.3	Dynamic
Delete	10.4.16.72	0000.7419.a200	vlan1-0	port1.0.3	Dynamic

Figure 121. ARP Table Page

The following fields are displayed:

- IP Address**— Indicates the IP address of the host that is connected to the switch.
- MAC Address**— Indicates MAC address of the host.
- Vlan**— Indicates the ID number of the VLAN where the host is a member.
- Interface**— Indicates the port number where the host is connected.
- Type**— Indicates the type of the ARP entry: static or dynamic.

Adding a Static ARP Entry

To add a static ARP entry, do the following:

1. Select the **Layer 3** tab.

The Layer 3 tab is displayed. See Figure 120 on page 293.

2. From the Layer 3 tab, select **ARP Table**.

The ARP table is displayed. See Figure 121 on page 293.

3. Click **Add**.

The Add Static ARP Page is displayed. See Figure 122.

The screenshot shows the 'Add Static ARP' page of the AT-8100S/24POE web interface. The page has fields for IP Address, MAC Address, VLAN, and Port, with an 'Add' button. A warning message box is visible on the right side of the page.

Warning: include
(ip4_interface_help.html)
function include: failed to open
stream: No such file or directory
in /var/www/html/add_arp_table.php
on line 125

Warning: include()
function include:
Failed opening
'ip4_interface_help.html' for inclusion
(include_path='...')
in /var/www/html/add_arp_table.php
on line 125

Figure 122. Add Static ARP Page

4. Enter the following settings:

- IP Address**— Enter the IPv4 address of the host to create an ARP entry.
- MAC Address**— Enter the MAC address that is associated to the IP address.
- VLAN**— Select a VLAN that the port belong to. The port is where the host is connected.

- **Port**— Enter a port ID where the host is connected to, for example, port1.0.8.

5. Click **Add**.
6. Click **SAVE** to save your changes to the startup configuration file.

Deleting ARP Entries

To delete a static ARP entry, do the following:

1. Select the Layer 3 tab.

The Layer 3 tab is displayed. See Figure 120 on page 293.

2. From the Layer 3 tab, select **ARP Table**.

The ARP table is displayed. See Figure 121 on page 293.

3. Do one of the following:

- To clear all of the dynamic ARP entries in the ARP address table, click Clear Dynamic.
- To delete a specific ARP entry, click Delete next to the IP address that you want to delete.

Chapter 25

LLDP and LLDP-MED

This chapter provides a brief description of the Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) features and explains how to enable these features on the switch. See the following sections:

- “Overview” on page 300
- “Enabling and Configuring LLDP on the Switch” on page 302
- “Disabling LLDP on the Switch” on page 305
- “Configuring LLDP on a Port” on page 306
- “Selecting LLDP TLVs on a Port” on page 308
- “Setting a Location Entry for the LLDP-MED Location TLV” on page 312
- “Assigning LLDP Locations to a Port” on page 322
- “Selecting LLDP-MED TLVs on a Port” on page 324
- “Displaying LLDP Neighbor Information” on page 327
- “Displaying LLDP Statistics” on page 329
- “Displaying Location Entries” on page 332
- “Displaying LLDP and LLDP-MED Settings” on page 335

For more information about the LLDP and LLDP-MED features, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- LLDP and LLDP-MED
- LLDP and LLDP-MED Commands

Overview

Link Layer Discovery Protocol (LLDP) and Link Layer Discovery Protocol for Media Endpoint Devices (LLDP-MED) allow Ethernet network devices such as switches and routers to receive and/or transmit device-related information to directly connected devices on the network that are also using the protocols, and store the information that is learned about other devices. The data sent and received by LLDP and LLDP-MED are useful for many reasons. The switch can discover other devices directly connected to it. Neighboring devices can use LLDP to advertise some parts of their Layer 2 configuration to each other, enabling some types of misconfiguration to be more easily detected and corrected.

LLDP is a “one hop” protocol. LLDP information can only be sent to and received by devices that are directly connected to each other, or connected via a hub or repeater. Devices that are directly connected to each other are called *neighbors*. Advertised information is not forwarded on to other devices on the network. In addition, LLDP is a one-way protocol. That is, the information transmitted in LLDP advertisements flows in one direction only, from one device to its neighbors, and the communication ends there. Transmitted advertisements do not solicit responses and received advertisements do not solicit acknowledgements. LLDP cannot solicit any information from other devices. LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static port trunks or LACP trunks, but not on the trunks themselves, and on switch ports that belong to VLANs, but not on the VLANs themselves.

Each port can be configured to transmit local information, receive neighbor information, or both. LLDP transmits information as packets called LLDP Data Units (LLDPDUs). An LLDPDU consists of a set of Type-Length-Value elements (TLV), each of which contains a particular type of information about the device or port transmitting it.

A single LLDPDU contains multiple TLVs. Each TLV includes a single type of information, such as its device ID, type, or management addresses, in a standardized format.

The TLVs are grouped as follows:

- Mandatory LLDP TLVs:

Chassis ID, Port ID, and Time to Live (TTL) that are Included in an LLDPDU by default.

- Optional LLDP TLVs:

You can select LLDP TLVs that are included in an LLDPDU. The switch sends selected TLVs along with the mandatory TLVs in an LLDPDU.

Optional LLDP-MED TLVs

You can select LLDP-MED TLVs that are included in an LLDPDU. The switch sends selected TLVs along with the mandatory TLVs in an LLDPDU.

Enabling and Configuring LLDP on the Switch

To enable LLDP and set the basic LLDP configuration to the switch, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123.



Figure 123. Discovery & Monitoring Tab

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears to the right.

3. From the LLDP tab, select the **Basic Configuration** tab.

The LLDP Configuration page is displayed. See Figure 124 on page 303.

LLDP Configuration

HELP

Status— Enable or disable LLDP on the switch. By default, LLDP is disabled.

Timer— Enter the transmit interval of LLDP advertisements. The transmit interval must be at least four times the transmission delay timer (Tx Delay). The range is 5 to 32,768 seconds. The default value is 30 seconds.

Fast start Count— Enter a fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from the port when it begins sending LLDP-MED.

Holdtime Multiplier— Enter the holdtime multiplier for LLDP advertisements. The range is 2 to 10. The default value is 4.

Non Strict Med TLV Order Check— A checked checkbox.

Notification Interval— Enter the notification interval. Range: 5-3600, Default: 5.

Reinit— Enter the reinit value. Range: 1-10, Default: 2.

Tx Delay— Enter the transmission delay timer. Range: 1-8192, Default: 2.

Total Neighbors— 0

Neighbors Last Update— 6h:26m:16s

Apply

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 124. LLDP Configuration Page

4. Change the following fields as needed:

- Status**— Enable LLDP on the switch. By default, LLDP is disabled.
- Timer**— Enter the transmit interval of LLDP advertisements. The transmit interval must be at least four times the transmission delay timer (Tx Delay). The range is 5 to 32,768 seconds. The default value is 30 seconds.
- Fast Start Count**— Enter a fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from the port when it begins sending LLDP-MED.

advertisements, for instance when it detects a new LLDP-MED capable device. The default value is 3.

- Holdtime Multiplier**— Enter a holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) the switch advertises to the neighbors. The range is 2 to 10.
- Non Strict Med TLV Order Check**— Check the checkbox to set the switch to accept LLDP-MED advertisements even if the TLVs are not in the standard order, as specified in ANSI/TIA-1057. This configuration is useful if the switch is connected to devices that send LLDP-MED advertisements in which the TLVs are not in the standard order. By default, this field is selected.
- Notification Interval**— Enter a notification interval. This is the minimum interval between LLDP SNMP notifications (traps). The range is 5 to 3,600 seconds.
- Reinit**— Enter a reinitialization delay. This is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized. The range is 1 to 10 seconds.
- Tx Delay**— Enter a transmission delay. This is the minimum time interval between transmissions of advertisements due to changes in LLDP local information. The range is 1 to 8192 seconds.
- Total Neighbors**— Indicates the number of LLDP neighbors the switch has discovered on all its ports.
- Neighbors Last Update**— Indicates the time since the LLDP neighbor table was last updated.

5. Click **Apply**.
6. Click **SAVE** to save your changes to the startup configuration file.

Disabling LLDP on the Switch

To disable the LLDP feature on a switch, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears to the right.

3. From the LLDP tab, select the **Basic Configuration** tab.

The LLDP Configuration page is displayed. See Figure 124 on page 303.

4. Use the pull-down menu next to the **Status** field to select “Disabled.”

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Configuring LLDP on a Port

To assign LLDP to a port, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP** and then select **Port Configurations**.

The LLDP Port Config page is displayed. See Figure 125.

	Interface	Notification	Adv. Transmit	Adv. Received	MED Notifications
Edit	port1.0.1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Edit	port1.0.2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Edit	port1.0.3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Edit	port1.0.4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Edit	port1.0.5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Edit	port1.0.6	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Edit	port1.0.7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Edit	port1.0.8	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Figure 125. LLDP Port Config Page

3. Select **Edit** next to the port that you want to modify.

The Modify LLDP Port Configuration page is displayed. See Figure 126 on page 307.



Figure 126. Modify LLDP Port Configuration Page

4. Change the settings as needed:

- Interface**— Indicates the port ID.
- Notifications**— Check the checkbox to activate the switch to send LLDP-MED topology change notifications when a device is connected to or disconnected from the port. By default, this field is not selected.
- Advertisement Transmit**— Check the checkbox to activate the port to send LLDP advertisements. A port configured to transmit LLDP advertisements sends the mandatory TLVs and any optional LLDP TLVs they have been specified to send. By default, this field is selected.
- Advertisement Receive**— Check the checkbox to activate the port to accept LLDP advertisements. A port configured to receive LLDP advertisements accepts all advertisements from their neighbors. By default, this field is selected.
- Med Notifications**— Check the checkbox to activate the switch to send LLDP-MED topology change notifications when a device is connected to or disconnected from the port. By default, this field is not selected.

5. Click **Apply**.

Selecting LLDP TLVs on a Port

To enable LLDP TLV, do the following:

1. Select the **Discovery & Monitoring** tab.

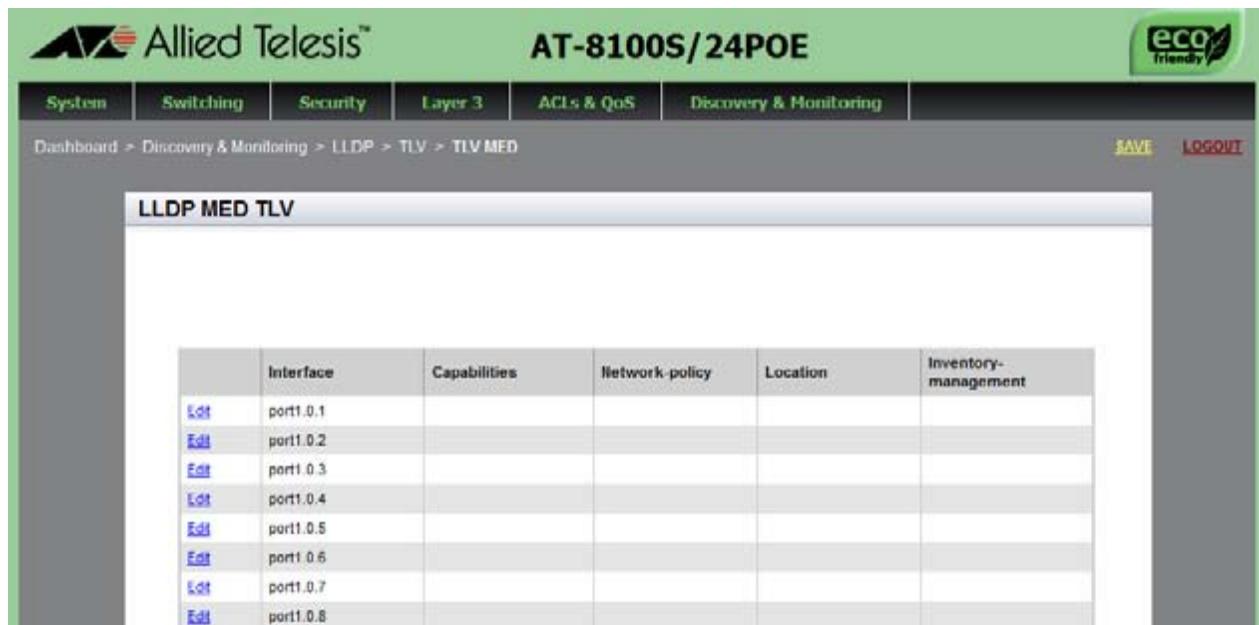
The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab is displayed.

3. From the LLDP tab, select **TLV**.

The LLDP TLV tab is displayed in Figure 127.



The screenshot shows the web interface for the Allied Telesis AT-8100S/24POE switch. The top navigation bar includes tabs for System, Switching, Security, Layer 3, ACLs & QoS, Discovery & Monitoring, and a highlighted Discovery & Monitoring tab. Below the tabs, the URL is shown as Dashboard > Discovery & Monitoring > LLDP > TLV > TLV MED. On the right, there are buttons for SAVE and LOGOUT. The main content area is titled 'LLDP MED TLV' and contains a table with the following data:

	Interface	Capabilities	Network-policy	Location	Inventory-management
Edit	port1.0.1				
Edit	port1.0.2				
Edit	port1.0.3				
Edit	port1.0.4				
Edit	port1.0.5				
Edit	port1.0.6				
Edit	port1.0.7				
Edit	port1.0.8				

Figure 127. LLDP TLV Tab

4. Move your cursor to the right and select **TLV** again.

The LLDP TLV page is displayed. See Figure 128 on page 309.

	Interface	Port Description	System Name	System Description	System Capabilities	Management Address	Port Vlan	Port And Protocol Vlans	Vlan Names	Protocol Ids	MAC Phy Config	Power Management	Link Aggregation	Max Frame Size
Edit	port1.0.1													
Edit	port1.0.2													
Edit	port1.0.3													
Edit	port1.0.4													
Edit	port1.0.5													
Edit	port1.0.6													

Figure 128. LLDP TLV Page

- Click **Edit** next to the port that you want to modify.

The Modify LLDP TLV page is displayed. See Figure 129 on page 310.

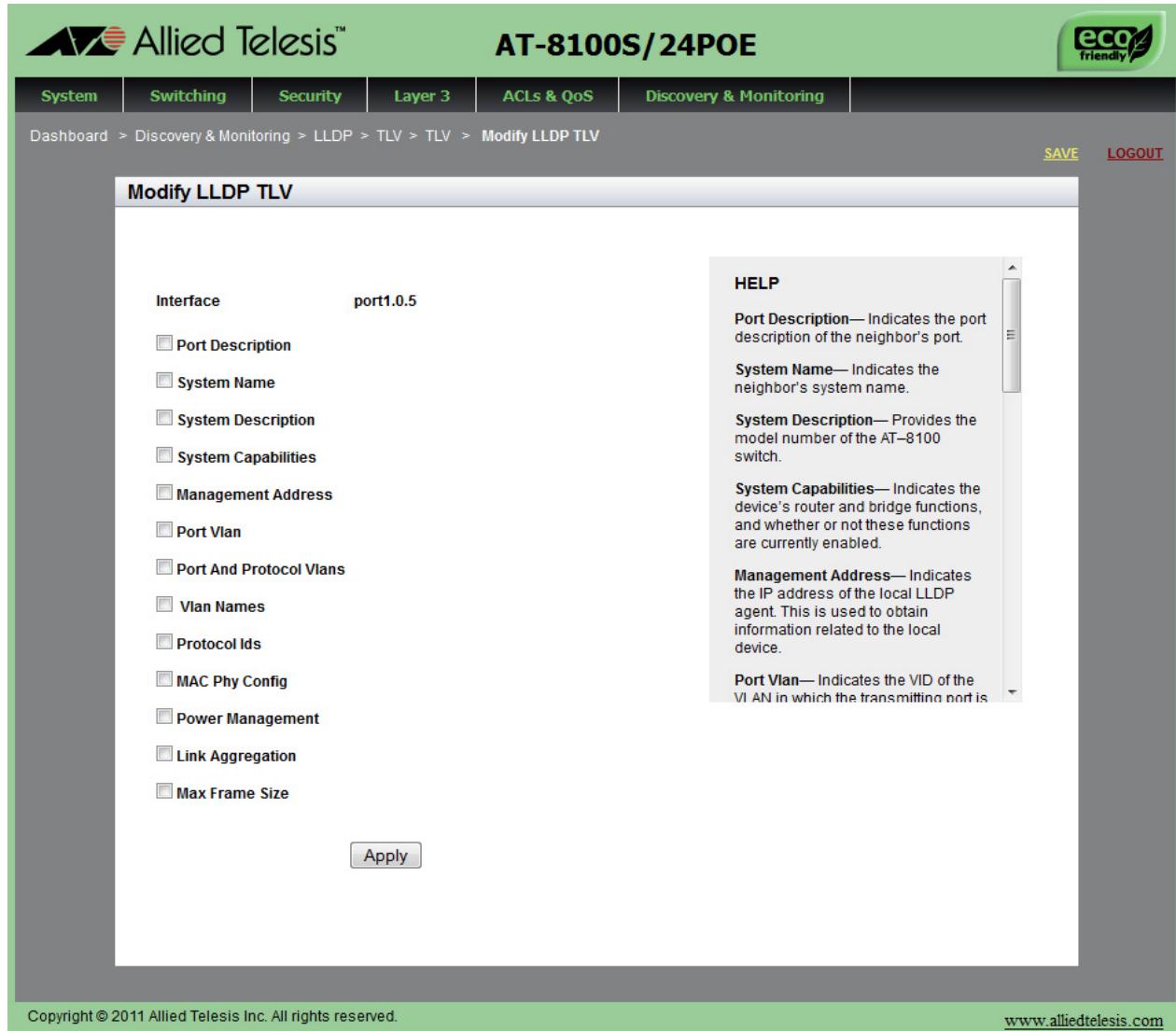


Figure 129. Modify LLDP TLV Page

6. Change the settings as needed:

- Interface**— Indicates the port ID.
- Port Description**— Check the checkbox to select the port description to be included in LLDPDUs.
- System Name**— Check the checkbox to select the system name to be included in LLDPDUs.
- System Description**— Check the checkbox to select the model number of the AT-8100 switch to be included in LLDPDUs.
- System Capabilities**— Check the checkbox to include the device's capabilities, such as router or bridge, and information whether or not these functions are currently enabled in LLDPDUs.

- Management Address**— Check the checkbox to select the IP address of the local LLDP agent to be included in LLDPDUs. Indicates.
- Port VLAN**— Check the checkbox to select the VID of the untagged VLAN in which the transmitting port a member to be included in LLDPDUs.
- Port and Protocol VLANs**— Check the checkbox to select information whether the device supports protocol VLANs and, if it does, the protocol VLAN identifiers to be included in LLDPDUs.
- VLAN Names**— Check the checkbox to select a list of the names of the VLANs in which the transmitting port is either an untagged or tagged member to be included in LLDPDUs.
- Protocol IDs**— Check the checkbox to select a list of protocol IDs that are accessible through the port to be included in LLDPDUs. For instance:
 - 9000 (Loopback)
 - 0026424203000000 (STP, RSTP, or MSTP)
 - 888e01 (802.1x)
 - AAAA03 (EPSR)
 - 88090101 (LACP)
 - 00540000e302 (Loop protection)
 - 0800 (IPv4)
 - 0806 (ARP)
 - 86dd (IPv6)
- MAC Phy Config**— Check the checkbox to select the physical layer information, including the link speed, duplex mode, and Auto-Negotiation setting to be included in LLDPDUs.
- Power Management**— Check the checkbox to select the power via MDI capabilities of the port to be included in LLDPDUs.
- Link Aggregation**— Check the checkbox to include information whether the port is capable of link aggregation and, if so, whether it is currently a member of an aggregator in LLDPDUs.
- Max Frame Size**— Check the checkbox to include the maximum supported frame size of the port in LLDPDUs. This field is not adjustable on the switch.

7. Click **Apply**.
8. Click **SAVE** to save your changes to the startup configuration file.

Setting a Location Entry for the LLDP-MED Location TLV

You can define location information about a network device as a LLDP-MED TLV and include the TLV in an LLDPDU, which the switch sends to its neighbors. Unlike some of the other LLDP-MED LLDP TLVs, such as capabilities and network policy TLVs, which have pre-set values, a location TLV must be specified before a port sends it to the neighbors.

To include location information in LLDPDUs, you must create a location entry with the relevant location information, apply it to one or more ports on the switch, and then specify a port to include the location TLV-MED in LLDPDUs.

The procedures in this section allow you to create LLDP-MED Civic, Coordinate, and ELIN location entries. See the following:

- ❑ “Creating a Civic Location Entry” on page 312
- ❑ “Creating a Coordinate Location” on page 316
- ❑ “Creating an Emergency Location Identification Number (ELIN) Location” on page 319

Note

To apply a location entry to a port, see “Assigning LLDP Locations to a Port” on page 322. To specify a port to include a location LLDP-MED TLVs, see “Selecting LLDP-MED TLVs on a Port” on page 324.

Creating a Civic Location Entry

To create an the LLDP Civic Location, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, select **Locations**.

The Locations tab is displayed. See Figure 130 on page 313.



Figure 130. Locations Tab

4. From the Locations tab, select **Civic**.

The LLDP Civic Location page is displayed. See Figure 131.

The screenshot shows the 'LLDP Civic Location' page. At the top, the ID is set to 101. Below the table, there are buttons for 'Delete', 'Edit', and 'Add'. The table lists the following location details:

Country	US	Building
State	CA	Unit
County	Santa Clara	Floor
City	San Jose	Room
Division		Place Type
Neighborhood		Postal Community Name
Street Group		Post Office Box
Leading Street Direction		Additional Code
Trailing Street Suffix		Seat
Street Suffix		Primary Road Name
House Number		Road Section
House Number Suffix		Branch Road Name
Landmark		Sub Branch Road Name
Additional Information		Street Name Pre Modifier
Name		Street Name Post Modifier
Postal Code		

Figure 131. LLDP Civic Location Page

5. Click **Add**.

The LLDP Civic Location Page is displayed. See Figure 132.

System Switching Security Layer 3 ACLs & QoS Discovery & Monitoring

AT-8100S/24POE

eco friendly

Dashboard > Discovery & Monitoring > LLDP > LLDP Civic Location List > Modify LLDP Civic Location

SAVE LOGOUT

Modify LLDP Civic Location

HELP

You must provide values for the Id and Country fields. The remaining fields are optional. Each field can contain up to 255 characters.

ID— Enter an Id number that indicates the civic location.

Country— Enter the country code for this civic location. The Country field must contain two uppercase characters, for example, "US."

Click **Apply** to save your changes to the running configuration file.

Please refer to the *AlliedWare Plus Web Browser User's Guide* for configuration instructions.

ID	101
Country	US
State	CA
County	Santa Clara
City	San Jose
Division	
Neighborhood	
Street Group	
Leading street Direction	
Street Suffix	
House Number	
House Number Suffix	
Landmark	
Additional Information	
Name	
Postal Code	
Building	
Unit	
Floor	
Room	
Place Type	
Postal Community Name	
Post Office Box	
Additional Code	
Seat	
Primary Road Name	
Road Section	
Branch Road Name	
Sub Branch Road Name	
Street Name Pre Modifier	
Street Name Post Modifier	

Apply

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 132. LLDP Civic Location Page— Modify

6. Enter the **ID** and **Country** fields:

- ID**— Enter an LLDP Civic Location ID. The range is 1 to 256. (This range is separate from the ranges for coordinate and ELIN entries.)
- Country**— Enter the country code. It must contain two uppercase characters (for example, US or FR).

Note

You must define the ID and Country fields. The remaining fields are optional.

7. Enter the ID and the following fields as needed:

Note

Each field can contain up to 255 characters. Spaces are not allowed.

The following list shows examples:

- State**— CA
- County**— Santa-Clara
- City**— San-Jose
- Division**— North-Park
- Neighborhood**— Parkside
- Street Group**— Addison
- Leading Street Direction**— West
- Trailing Street Suffix**— Avenue
- Street Suffix**— Blvd
- House Number**— 401
- House Number Suffix**— C
- Landmark**— City-library
- Additional Information**— Updated-Oct-2011
- Name**— J-Smith
- Postal Code**— 95134
- Building**— 02
- Unit**— A11
- Floor**— 4
- Room**— 402
- Place Type**— Business-district
- Postal Community Name**— Lyton

- Post Office Box**— 102
- Additional Code**— 1234
- Seat**— cube-411a
- Primary Road Name**— Zanker
- Road Selection**— North
- Branch Road Name**— State-Lane
- Sub Branch Road Name**— Boulder-Creek-Avenue
- Street Name Pre Modifier**— West
- Street Name Pre Modifier**— Div

8. Click **Apply**.
9. Click **SAVE** to save your changes to the startup configuration file.

Creating a Coordinate Location

To create an LLDP Coordinate Location, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, select **Locations**.

The Locations tab is displayed. See Figure 130 on page 313.

4. From the Location tab, select **Coordinates**.

The LLDP Coordinate Location page is displayed. See Figure 133 on page 317.

Dashboard > Discovery & Monitoring > LLDP > Locations > Coordinates

SAVE [LOGOUT](#)

LLDP Coordinate Location

	ID	Latitude	Latitude Resolution	Longitude	Longitude Resolution	Altitude	Altitude Resolution	Datum
Delete Edit	1	90.000000	16	180.000000	16	200.000000 Meters		WGS84

Copyright © 2011 Allied Telesis Inc. All rights reserved. www.alliedtelesis.com

Figure 133. LLDP Coordinate Location Page

5. From the LLDP Coordinate Location page, click Add.

The LLDP Coordinate Location page is displayed. See Figure 134 on page 318.

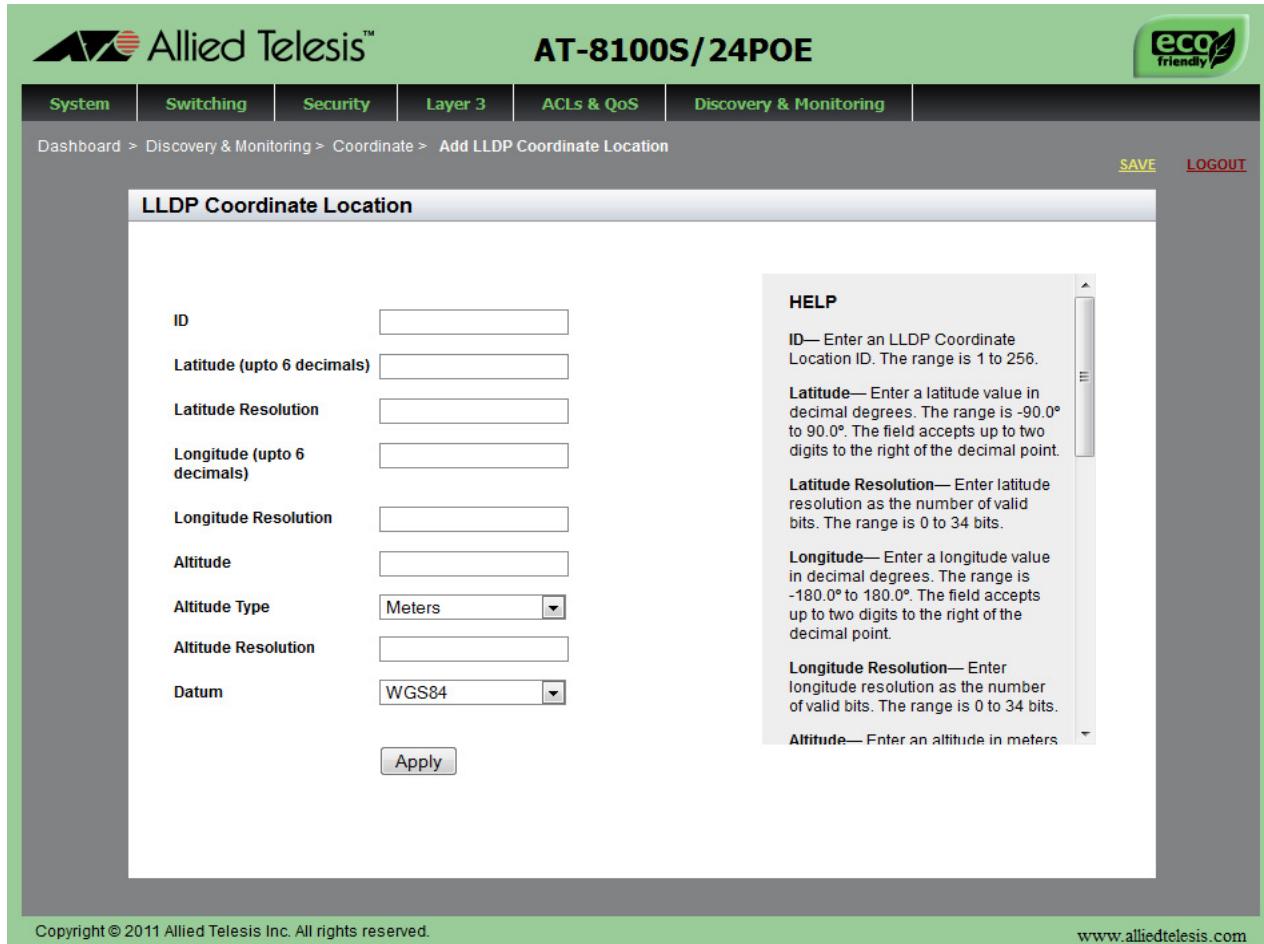


Figure 134. LLDP Coordinate Location Page—Modify

6. Specify the following fields as needed:

- ID**—Enter an LLDP Coordinate Location ID. The range is 1 to 256. (This range is separate from the ranges for civic and ELIN entries.)
- Latitude**—Enter a latitude value in decimal degrees. The range is -90.0° to 90.0° . The field accepts up to two digits to the right of the decimal point.
- Latitude Resolution**—Enter latitude resolution as the number of valid bits. The range is 0 to 34 bits.
- Longitude**—Enter a longitude value in decimal degrees. The range is -180.0° to 180.0° . The field accepts up to two digits to the right of the decimal point.
- Longitude Resolution**—Enter longitude resolution as the number of valid bits. The range is 0 to 34 bits.

- Altitude**— Enter an altitude in meters or floors. For the altitude in meters, the range is -2097151.0 to 2097151.0 meters. The parameter accepts up to eight digits to the right of the decimal point. For altitude in the number of floors, the range is -2097151.0 to 2097151.0. Use the **Altitude Type** field to specify meters or floors.
- Altitude Type**— Choose between meters and floors.
- Altitude Resolution**— Enter altitude resolution as the number of valid bits. The range is 0 to 30 bits.
- Datum**— Select the geodetic system (or datum) of the coordinates. Choose one of the following:

WGS84: World Geodetic System 1984

NAD83_NAVD: North American vertical datum 1983

NAD83_MLLW: Mean lower low water datum 1983

7. Click **Apply**.

Creating an Emergency Location Identification Number (ELIN) Location

The ELIN TLV specifies the location of a network device by its Emergency Location Identifier Number (ELIN).

To create an LLDP ELIN location, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, select **Locations**.

The Locations tab is displayed. See Figure 130 on page 313.

4. From the Location tab, select **ELIN**.

The LLDP ELIN Location List page is displayed. See Figure 135 on page 320.



Figure 135. LLDP ELIN Location List Page

- From the LLDP ELIN Location page, click Add.

The LLDP ELIN Location page is displayed. See Figure 136.

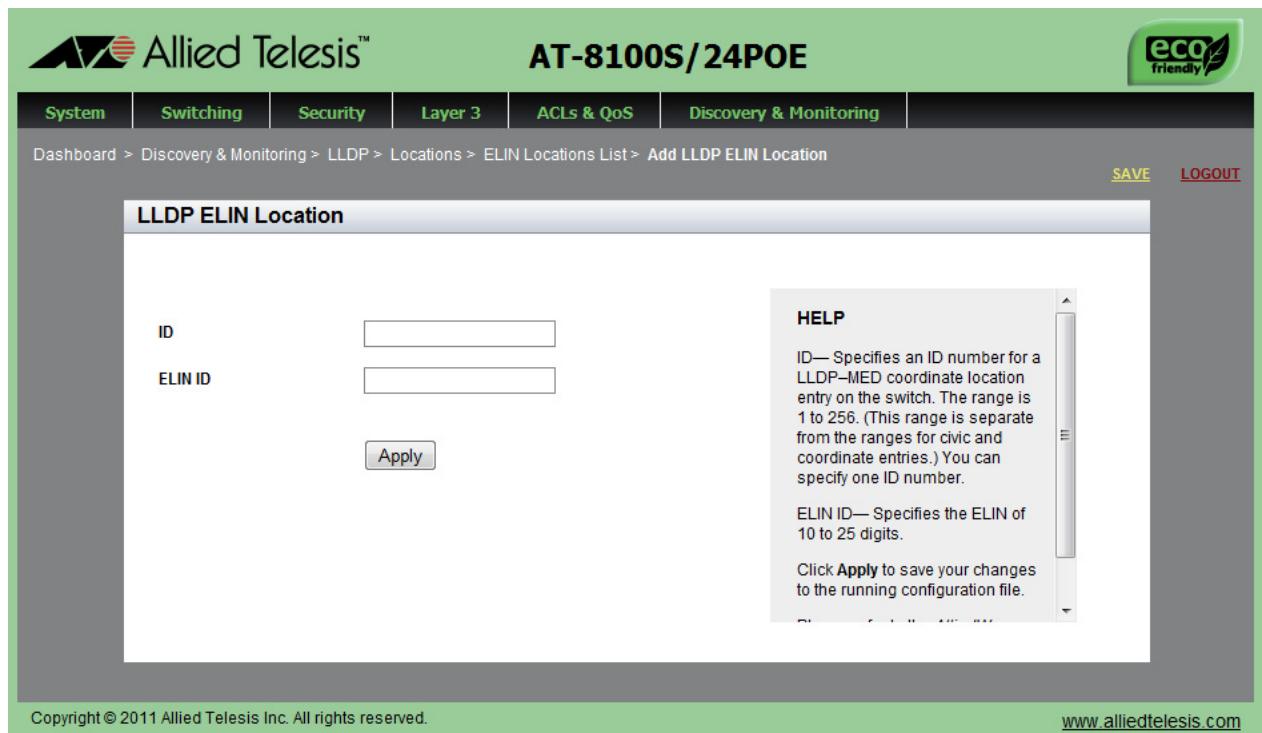


Figure 136. LLDP ELIN Location Page

6. Enter values in the following fields:

- ID**— Enter an ID number for a LLDP-MED coordinate location entry on the switch. The range is 1 to 256. (This range is separate from the ranges for civic and coordinate entries.)
- ELIN-LOCATION**— Enter an ELIN location of 10 to 25 digits.

7. Click **Apply**.

Assigning LLDP Locations to a Port

Use a Civic, Coordinate, or ELIN location IDA port location to assign to a port. You must create these location IDs *before* you assign a port location to a port. For instructions to create location IDs, see “Setting a Location Entry for the LLDP-MED Location TLV” on page 312.

To set an LLDP port location, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, select **Port Locations**.

The LLDP Port Location page is displayed. See Figure 137.

	Interface	Civic Location ID	Coordinate Location ID	ELIN Location ID
Edit	port1.0.1			
Edit	port1.0.2			
Edit	port1.0.3			
Edit	port1.0.4			
Edit	port1.0.5			
Edit	port1.0.6			
Edit	port1.0.7			
Edit	port1.0.8			

Figure 137. LLDP Port Location Page

4. Click **Edit** next to the port that you want to modify.

The Modify LLDP Port Location page is displayed. See Figure 138 on page 323.

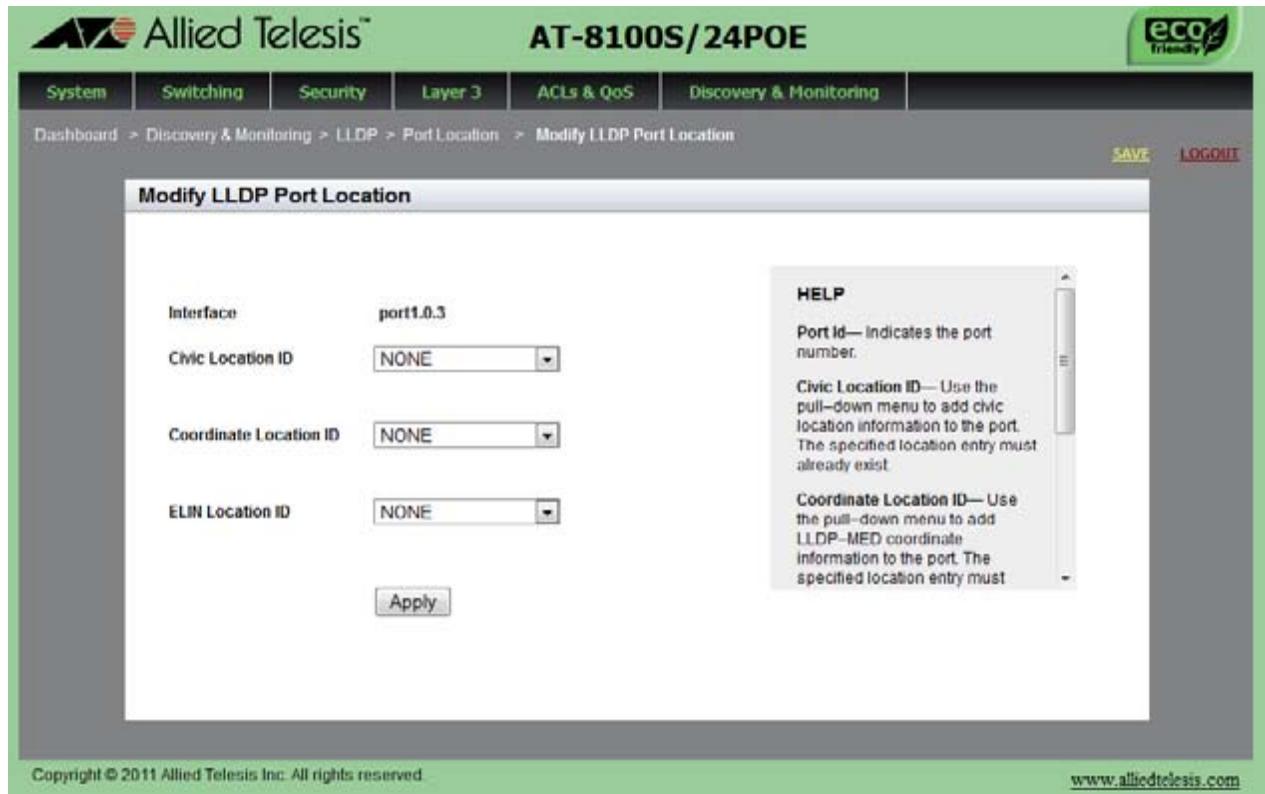


Figure 138. Modify LLDP Port Location Page

5. Select values in the fields as needed:
 - Interface** — Indicates the port ID.
 - Civic Location ID** — Select a Civic Location ID from the pull-down menu. By default, none is selected.
 - Coordinate Location ID** — Select a Coordinate Location ID from the pull-down menu. By default, none is selected.
 - ELIN Location ID** — Select an ELIN Location ID from the pull-down menu. By default, none is selected.
6. Click **Apply**.
7. Click **SAVE** to save your changes to the startup configuration file.

Selecting LLDP-MED TLVs on a Port

To enable LLDP-MED TLV, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP** and then select **TLV**.

The LLDP TLV tab is displayed. See Figure 127 on page 308.

3. From the LLDP TLV tab, select **TLV-MED**.

The LLDP-MED TLV page is displayed. See Figure 139.

	Interface	Capabilities	Network-policy	Location	Inventory-management
Edit	port1.0.1				
Edit	port1.0.2				
Edit	port1.0.3				
Edit	port1.0.4				
Edit	port1.0.5				
Edit	port1.0.6				
Edit	port1.0.7				
Edit	port1.0.8				

Figure 139. LLDP-MED TLV Page

4. Click **Edit** next to the port that you want to modify.

The Modify LLDP-MED TLV page is displayed. See Figure 140 on page 325.



Figure 140. Modify LLDP-MED TLV Page

5. Change the fields as needed:

- Interface**— Indicates the port ID.
- Capabilities**— Check the checkbox to select the capabilities to be included in LLDPDUs.
- Network-policy**— Check the checkbox to select the network policy TLV to be included in LLDPDUs. The network policy TLV includes the network policy information specified on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data:
 - Voice VLAN ID
 - Voice VLAN Class of Service (CoS) priority
 - Voice VLAN Diffserv Code Point (DSCP)

- Location**— Check the checkbox to select the location TLV to be included in LLDPDUs. The location TLV is in one or more of the following formats:
 - Civic location
 - Coordinate location
 - Emergency Location Identification Number (ELIN)
- Inventory-management**— Check the checkbox to select the current hardware and the software information to be included in LLDPDUs. This information is identical on every port on the switch:
 - Hardware Revision
 - Firmware Revision
 - Software Revision
 - Serial Number
 - Manufacturer Name
 - Model Name
 - Asset ID

6. Click **Apply**.

7. Click **SAVE** to save your changes to the startup configuration file.

Displaying LLDP Neighbor Information

To display LLDP Statistical information, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP** and then select **Neighbors**.

The LLDP Neighbors Information page is displayed. See Figure 141.

The screenshot shows the 'Discovery & Monitoring' tab selected in the top navigation bar. The 'Neighbors' sub-tab is also selected. The main content area is titled 'LLDP Neighbors Information'. It contains two sections: 'System Capability Codes' and 'LLDP-MED Device Class And Power Source Codes'. Below these sections is a table with columns for Port Id, Neighbor Chassis Id, Neighbor Port Name, Neighbor System Name, System Capabilities (with checkboxes for O, P, B, W, R, T, C, S), and Med Device class and Power Source Code (with checkboxes for C1, C2, C3, N, PSE, L, Both, Prim, UN, Ba). The table has a header row with these column names. At the bottom of the page, there is a copyright notice and a website address.

Figure 141. LLDP Neighbors Information Page

The following fields are displayed:

- Interface**— Indicates the port ID.
- Neighbor Chassis ID**— Indicates the ID number of the neighbor's chassis.
- Neighbor Port Name**— Indicates the neighbor's port number that sent the information.
- Neighbor System Name**— Indicates the neighbor's system name.
- System Capabilities**— Indicates capabilities that are supported and enabled on the neighbor. The System Capabilities codes are:

O = Other

P = Repeater

B= Bridge

W = Wireless Access Point

R = Router

T = Telephone

C= Cable Device

S = Station only

- **Med Device class and Power Source code**— Indicates whether or not the MED device Classes I through III are supported. Power Source code indicates the current power source which is either the Primary Power Source or the Backup Power Source. The codes are:

C1 = Class I

C2 = Class II

C3 = Class III

N = Network

L = Local

PSE = PoE

prim = Primary

UN = Unknown

Ba = Backup

Displaying LLDP Statistics

To display LLDP Statistics, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**
3. From the LLDP tab, select **Statistics**.

The LLDP Statistics page is displayed with the Port Statistics tab selected automatically. See Figure 142.

Port ID	Out Frames	In Frames	In Frames Errored	In Frames Dropped	Unrecognized TLVs	Discarded	New Entries	Deleted Entries	Dropped Entries	Ageout Entries
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0

Figure 142. LLDP Statistics Page with Port Statistics Tab

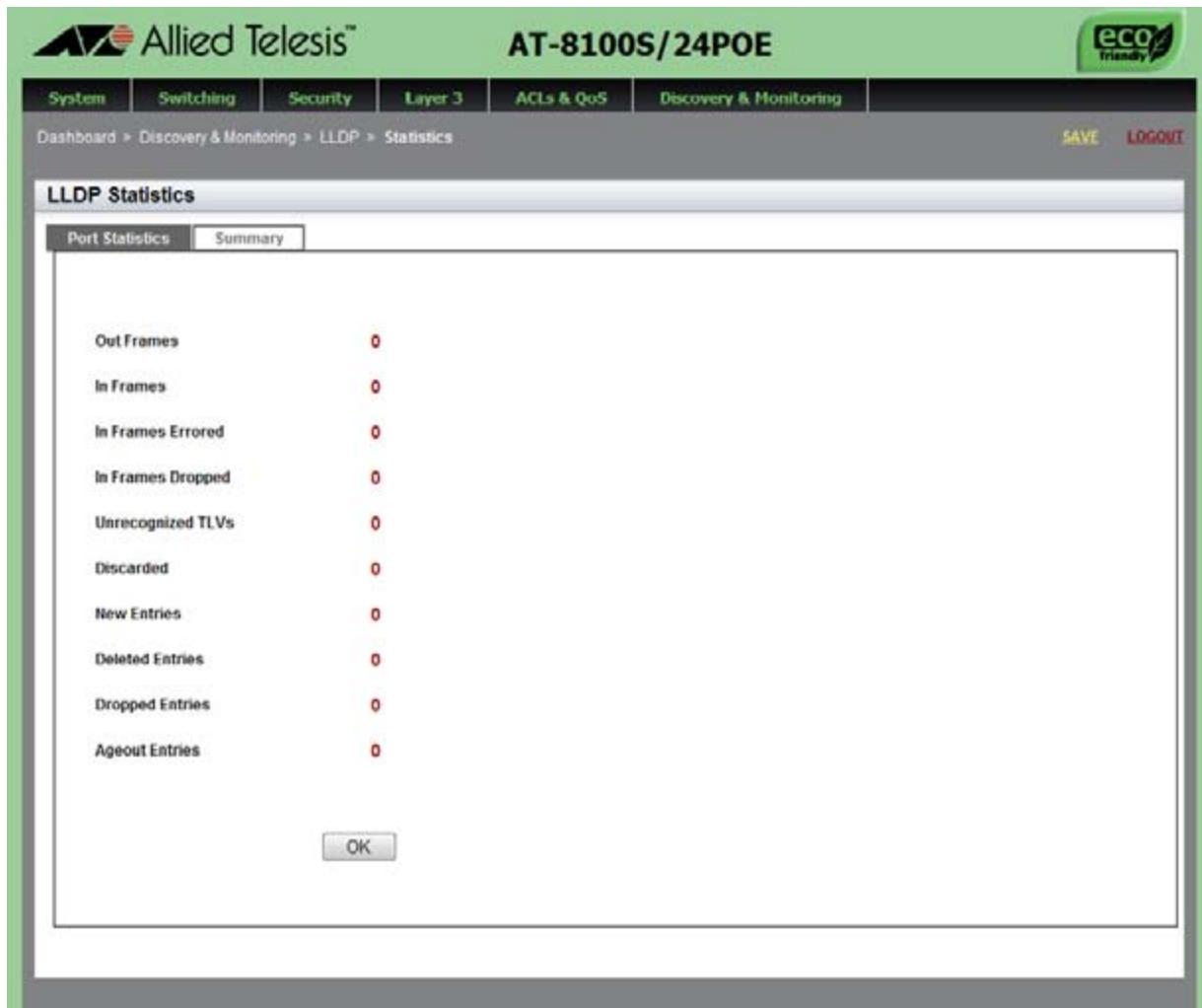
The following fields are displayed:

- Interface**— Indicates the port ID.
- Out Frames**— Indicates the number of LLDPDU frames transmitted.
- In Frames**— Indicates the number of LLDPDU frames received.
- In Frames Errored**— Indicates the number of invalid LLDPDU frames received.
- In Frames Dropped**— Indicates the number of LLDPDU frames received and discarded.
- Unrecognized TLVs**— Indicates the number of LLDP TLVs received that were unrecognized, but the TLV types were in the range of reserved TLV types.

- Discarded**— Indicates the number of discarded TLVs.
- New Entries**— Indicates the number of times the information advertised by neighbors has been inserted into the neighbor table.
- Deleted Entries**— Indicates the number of times the information advertised by neighbors has been removed from the neighbor table.
- Dropped Entries**— Indicates the number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
- Ageout Entries**— Indicates the number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

4. Select the **Summary** tab.

The LLDP Statistics Summary page is displayed. See Figure 143.



The screenshot shows the 'LLDP Statistics' page with the 'Summary' tab selected. The table lists the following statistics and their current values:

Statistic	Value
Out Frames	0
In Frames	0
In Frames Errorred	0
In Frames Dropped	0
Unrecognized TLVs	0
Discarded	0
New Entries	0
Deleted Entries	0
Dropped Entries	0
Ageout Entries	0

At the bottom of the table is an 'OK' button.

Figure 143. LLDP Statistics Page with Summary Tab

The fields are described in step 3. These fields list the statistics for all of the ports.

5. Click **OK** to return to the LLDP Statistics Page with the Port Statistics Tab selected.

Displaying Location Entries

To display the LLDP Civic, Coordinate, and ELIN locations, use the following procedures:

- “Displaying Civic Locations” on page 332
- “Displaying Coordinate Locations” on page 333
- “Displaying ELIN Locations” on page 334

For information about creating LLDP locations, see “Enabling and Configuring LLDP on the Switch” on page 302.

Displaying Civic Locations

To display a Civic Location, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, select **Locations**.

The Locations tab is displayed. See Figure 130 on page 313.

4. From the Locations tab, select **Civic**.

The LLDP Civic Location page is displayed. See Figure 132 on page 314.

The following fields are displayed:

- ID**
- Country**
- State**
- County**
- City**
- Division**
- Neighborhood**
- Street Group**
- Leading Street Direction**
- Trailing Street Suffix**
- Street Suffix**

- House Number**
- House Number Suffix**
- Landmark**
- Additional Information**
- Name**
- Postal Code**
- Building**
- Unit**
- Floor**
- Room**
- Place Type**
- Postal Community Name**
- Post Office Box**
- Additional Code**
- Seat**
- Primary Road Name**
- Road Selection**
- Branch Road Name**
- Sub Branch Road Name**
- Street Name Pre Modifier**
- Street Name Pre Modifier**

Displaying Coordinate Locations

To display a Coordinate Location, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, select **Locations**.

The Locations tab is displayed. See Figure 130 on page 313.

4. From the Locations tab, select **Coordinates**.

The LLDP Coordinate Location page is displayed. See Figure 134 on page 318.

The following fields are displayed:

- ID**— Indicates the LLDP Coordinate Location ID.
- Latitude**— Indicates the latitude value in decimal degrees.
- Latitude Resolution**— Indicates the latitude resolution as the number of valid bits.
- Longitude**— Indicates the longitude value in decimal degrees.
- Longitude Resolution**— Indicates the longitude resolution as the number of valid bits.
- Altitude**— Indicates the altitude.
- Altitude Resolution**— Indicates the altitude resolution as the number of valid bits.
- Datum**— Indicates the geodetic system (or datum) of the coordinates. The datum codes are:

WGS84: World Geodetic System 1984

NAD83-MLLW: Mean lower low water datum 1983

NAD83-NAVD: North American vertical datum 1983

Displaying ELIN Locations

To display an LLDP ELIN location, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, select **Locations**.

The Locations tab is displayed. See Figure 130 on page 313.

4. From the Location tab, select **ELIN**.

The LLDP ELIN Location page is displayed. See Figure 136 on page 320.

The following fields are displayed:

- ID**— Indicates an ID number for a LLDP-MED coordinate location entry on the switch.
- Elin ID**— Indicates the ELIN of 10 to 25 digits.

Displaying LLDP and LLDP-MED Settings

To display the LLDP Civic, Coordinate, and ELIN locations, use the following procedures:

- “Displaying the Basic LLDP Configuration” on page 335
- “Displaying LLDP Port Assignments” on page 336
- “Displaying Port Locations” on page 337
- “Displaying LLDP TLV” on page 337
- “Displaying LLDP-MED TLV” on page 339

For information about configuring LLDP and LLDP-MED, see “Assigning LLDP Locations to a Port” on page 322

Displaying the Basic LLDP Configuration

To display the basic LLDP configuration, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears to the right.

3. From the LLDP tab, select the **Basic Configuration** tab.

The LLDP Configuration page is displayed. See Figure 124 on page 303.

The following fields are displayed:

- Status**— Indicates whether LLDP is enabled or disabled on the switch.
- Timer**— Indicates the transmit interval.
- Fast Start Count**— Indicates the fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from a port when it begins sending LLDP-MED advertisements from a port, for instance when it detects a new LLDP-MED capable device.
- Holdtime Multiplier**— Indicates the holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) the switch advertises to the neighbors.
- Non Strict Med TLV Order Check**— Indicates whether the switch accepts LLDP-MED advertisements when the TLVs are not in the standard order, as specified in ANSI/TIA-1057.

- Notification Interval**— Indicates the notification interval. This is the minimum interval between LLDP SNMP notifications (traps).
- Reinit**— Indicates the reinitialization delay. This is the number of seconds that must elapse after LLDP is disabled on a port before it can be reinitialized.
- Tx Delay**— Indicates the transmission delay. This is the minimum time interval between transmissions of advertisements due to changes in LLDP local information.
- Total Neighbors**— Indicates the number of LLDP neighbors the switch has discovered on all its ports.
- Neighbors Last Update**— Indicates the time since the LLDP neighbor table was last updated.

Displaying LLDP Port Assignments

To display LLDP port assignments, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP** and then select **Port Configurations**.

The LLDP Port Config page is displayed. See Figure 125 on page 306.

The following fields are displayed:

- Interface**— Indicates the port ID.
- Notification**— Indicates whether the switch sends LLDP-MED topology change notifications when devices are connected to or disconnected from the specified ports.
- Adv. Transmit**— Indicates whether the port sends LLDP advertisements. Ports configured to transmit LLDP advertisements send the mandatory TLVs and any optional LLDP TLVs they have been specified to send.
- Adv. Receive**— Indicates whether the port accepts LLDP advertisements. Ports configured to receive LLDP advertisements accept all advertisements from their neighbors.
- Med Notification**— Indicates whether the switch sends LLDP-MED topology change notifications when devices are connected to or disconnected from the specified ports.

Displaying Port Locations

To display the LLDP port locations, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab appears on the right.

3. From the LLDP tab, select **Port Locations**.

The LLDP Port Location page is displayed. See Figure 137 on page 322.

The following fields are displayed.

- Interface**— Indicates the port ID.
- Civic Location ID**— Indicates the Civic location ID.
- Coordinate Location ID**— Indicates the coordinate location ID.
- ELIN Location ID**— Indicates the ELIN location ID.

Displaying LLDP TLV

To display the LLDP TLV settings, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP**.

The LLDP tab is displayed.

3. From the LLDP tab, select **TLV**.

The LLDP TLV tab is displayed in Figure 127 on page 308.

4. From the LLDP TLV tab, select **TLV** again.

The LLDP TLV page is displayed. See Figure 128 on page 309.

The following fields are displayed:

- Interface**— Indicates the port ID.
- Port Description**— Indicates the port description of the neighbor's port.
- System Name**— Indicates the neighbor's system name.
- System Description**— Indicates the model number of the AT-8100 switch.

- System Capabilities**— Indicates the device's router and bridge functions, and whether or not these functions are currently enabled.
- Management Address**— Indicates the IP address of the local LLDP agent. This is used to obtain information related to the local device.
- Port VLAN**— Indicates the VID of the VLAN in which the transmitting port is an untagged member.
- Port and Protocol VLANs**— Indicates whether the device supports protocol VLANs and, if it does, the protocol VLAN identifiers. This field is not supported on the AT-8100 switches.
- VLAN Names**— Lists the names of the VLANs in which the transmitting port is either an untagged or tagged member.
- Protocol IDs**— List of protocols that are accessible through the port, for instance:
 - 9000 (Loopback)
 - 0026424203000000 (STP, RSTP, or MSTP)
 - 888e01 (802.1x)
 - AAAA03 (EPSR)
 - 88090101 (LACP)
 - 00540000e302 (Loop protection)
 - 0800 (IPv4)
 - 0806 (ARP)
 - 86dd (IPv6)
- MAC Phy Config**— Indicates the speed and duplex mode of the port and whether the port was configured with Auto-Negotiation.
- Power Management**— Indicates the power via MDI capabilities of the port.
- Link Aggregation**— Indicates whether the port is capable of link aggregation and, if so, whether or not it is currently a member of an aggregator.
- Max Frame Size**— Indicates the maximum supported frame size the port can send. This field is not adjustable on the switch.

Displaying LLDP-MED TLV

To display LLDP-MED TLV settings, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 123 on page 302.

2. From the **Discovery & Monitoring** tab, select **LLDP** and then select **TLV**.

The LLDP TLV tab is displayed. See Figure 127 on page 308.

3. From the LLDP TLV tab, select **TLV-MED**.

The LLDP-Med TLV page is displayed. See Figure 139 on page 324.

The following fields are displayed:

- Interface**— Indicates the port ID.
- Capabilities**— Indicates the device's router and bridge functions, and whether or not these functions are currently enabled.
- Network-policy**— Indicates the network policy information specified on the port for connected media endpoint devices. The switch supports Application Type 1: Voice, including the following network policy for connected voice devices to use for voice data:
 - Voice VLAN ID
 - Voice VLAN Class of Service (CoS) priority
 - Voice VLAN Diffserv Code Point (DSCP)
- Location**— Indicates location information specified for the port, in one or more of the following formats:
 - Civic location
 - Coordinate location
 - Emergency Location Identification Number (ELIN)
- Inventory-management**— Indicates the current hardware platform and the software version, identical on every port on the switch:
 - Hardware Revision
 - Firmware Revision
 - Software Revision
 - Serial Number
 - Manufacturer Name

- Model Name

- Asset ID

Chapter 26

sFlow

This chapter provides a brief description of the sFlow feature and explains how to enable this feature on the switch and on a port.

See the following sections:

- “Overview” on page 342
- “Configuring sFlow on a Port” on page 344
- “Specifying an sFlow Collector” on page 346
- “Enabling sFlow on the Switch” on page 348
- “Displaying the sFlow Settings” on page 349

For more information about the sFlow feature, see the following chapters in the *AlliedWare Plus Management Software Version 2.2.4 Command Line Interface User’s Guide*:

- sFlow Agent
- sFlow Agent Commands

Overview

The sFlow agent allows the switch to gather data about the traffic on the ports and to send the data to sFlow collectors on your network for analysis. You can use the information to monitor the performance of your network or identify traffic bottlenecks.

The sFlow agent can gather two types of information about the traffic on the ports of the switch:

- Ingress packet samples
- Packet counters

Ingress Packet Samples

The sFlow agent can capture ingress packets on ports and send copies of the packets to sFlow collectors on your network for analysis. Depending on the capabilities of the collectors, packets can be scrutinized for source and destination MAC or IP addresses, protocol type, length, and so forth.

Packet sampling is activated by specifying sampling rates on the ports. This value defines the number of ingress packets from which the agent samples one packet. For example, a sampling rate of 1000 on a port prompts the agent to send one packet from every 1000 ingress packets to the designated sFlow collector. Different ports can have different rates.

Packet Counters

The agent can also gather and send data to a collector about overall information regarding the status and performance of the ports, such as speeds and status, and the statistics from the packet counters. The counters contain the number and types of ingress and egress packets handled by the ports since the switch or the counters were last reset. The agent can gather and send the following port status and counter information to a collector on your network:

- Port number
- Port type
- Speed
- Direction
- Status
- Number of ingress and egress octets
- Number of ingress and egress unicast packets
- Number of ingress and egress multicast packets
- Number of ingress and egress broadcast packets
- Number of ingress and egress discarded packets
- Number of ingress and egress packets with errors
- Number of ingress packets with unknown protocols

To configure the agent to forward these port statistics to the collectors, you have to specify polling rates, which define the maximum amount of time permitted between successive queries of the counters of a port by the agent.

Different ports can have different polling rates. Ports to which critical network devices are connected can be assigned low polling rates, so that the information on the collector is kept up-to-date. Ports connected to less critical devices can be assigned higher polling rates.

To increase its efficiency, the agent can send port status and counter information before the polling interval of a port times out. For example, if you define a polling interval of five minutes for a port, the agent, depending on its internal dynamics, may send the information to the collector before five minutes have actually elapsed.

sFlow Collectors

The sFlow agent on the switch can send port performance data to an sFlow collector on your network. The performance data from each port can be sent to one collector.

Guidelines

Here are the guidelines for the sFlow agent:

- You can specify just one sFlow collector.
- The sFlow collectors must be members of the same subnet as the management IP address of the switch, or must have access to it through routers or other Layer 3 devices.
- If the sFlow collectors are not a member of the same subnet as the management IP address of the switch, the switch must have a default gateway that specifies the first hop to reaching the collectors' subnet. For instructions, refer to Chapter 19, “Setting IPv4 and IPv6 Addresses” on page 229.
- The sFlow feature is not dependent on SNMP. You do not have to enable or configure SNMP on the switch to use the sFlow feature. In addition, you cannot use sFlow collectors to configure or manage SNMP.

Configuring sFlow on a Port

To configure the sFlow feature on a port, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 144.



Figure 144. Discovery & Monitoring Tab

2. From the **Discovery & Monitoring** tab, select **sFlow**.

The sFlow page is displayed with the Port Configurations tab selected. See Figure 145.

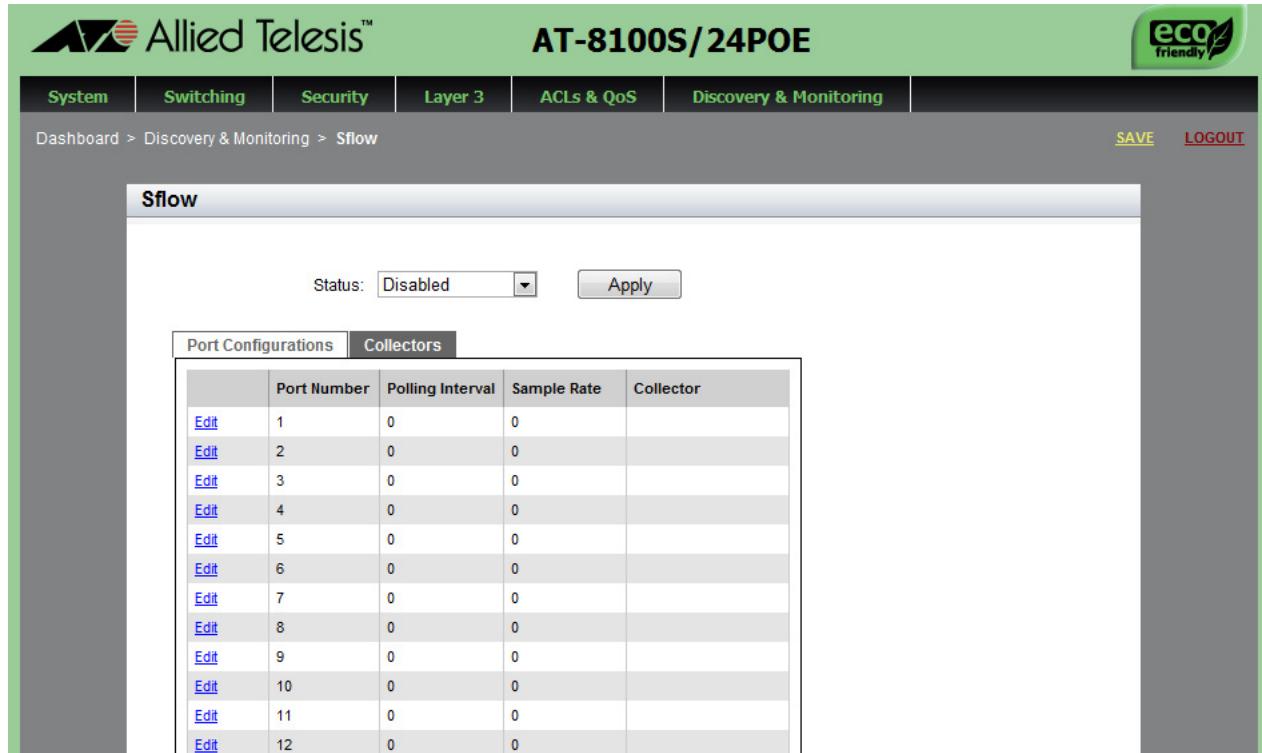


Figure 145. sFlow Page with the Port Configurations Tab

3. Click Edit next to the port that you want to modify.

The sFlow Port Modify page is displayed. See Figure 146.



Figure 146. sFlow Port Modify Page

4. Change the following fields as needed:

- Interface**— Indicates the port ID.
- Polling Interval**— Enter the polling interval for the port. This controls the maximum amount of time permitted between successive pollings of the packet counter on the port by the sFlow agent.
- Sample Rate**— Enter the packet sampling rate on the port. The sampling rate dictates the number of ingress packets from which one sample is taken on a port and sent by the agent to the sFlow collector. For example, a sample rate of 700 on a port means that one sample packet is taken for every 700 ingress packets. The possible values are 0 and 256 to 16,441,700 packets. Entering the value 0 disables packet sampling.

5. Click **Apply**.

6. Click **SAVE** to save your changes to the startup configuration file.

Specifying an sFlow Collector

Use this procedure to specify the IP address and the UDP port of an sFlow collector on your network. The packet sampling data and the packet counters are sent by the switch to the collector specified. You can specify only one collector.

To select the Collector tab from the sFlow page, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 144 on page 344.

2. From the **Discovery & Monitoring** tab, select **sFlow**.

The sFlow page is displayed with the Port Configurations tab selected. See Figure 145 on page 344.

3. From the sFlow page, select the **Collector** tab.

The sFlow page is displayed with the Collector Tab selected. See Figure 147.

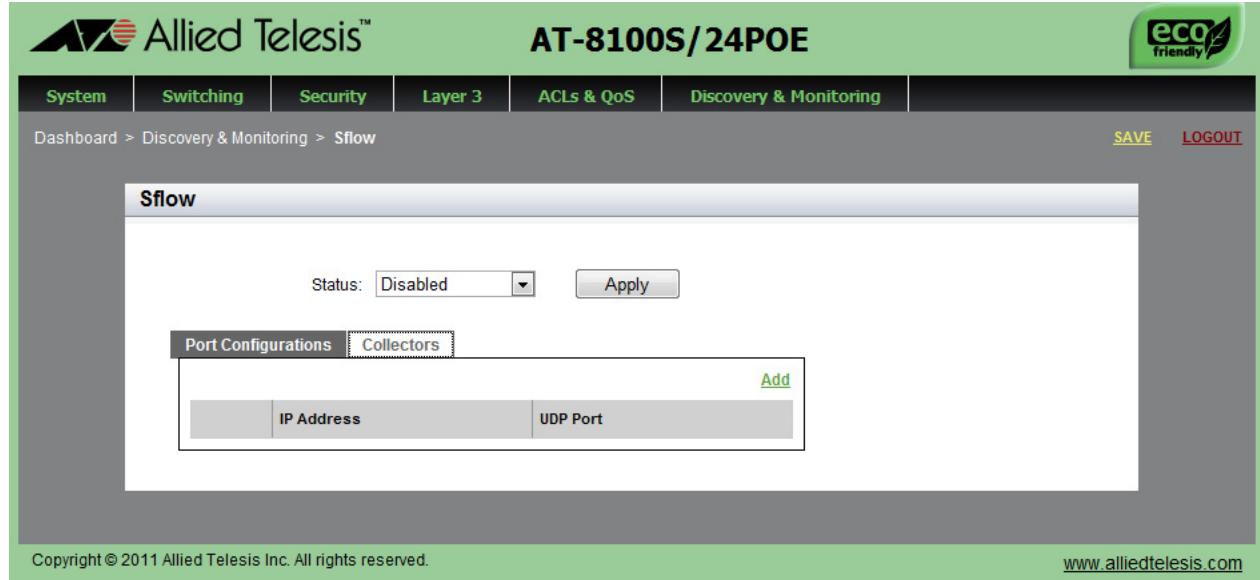


Figure 147. sFlow Page with Collectors Tab

4. Click Add.

The sFlow Collector page is displayed. See Figure 148 on page 347.

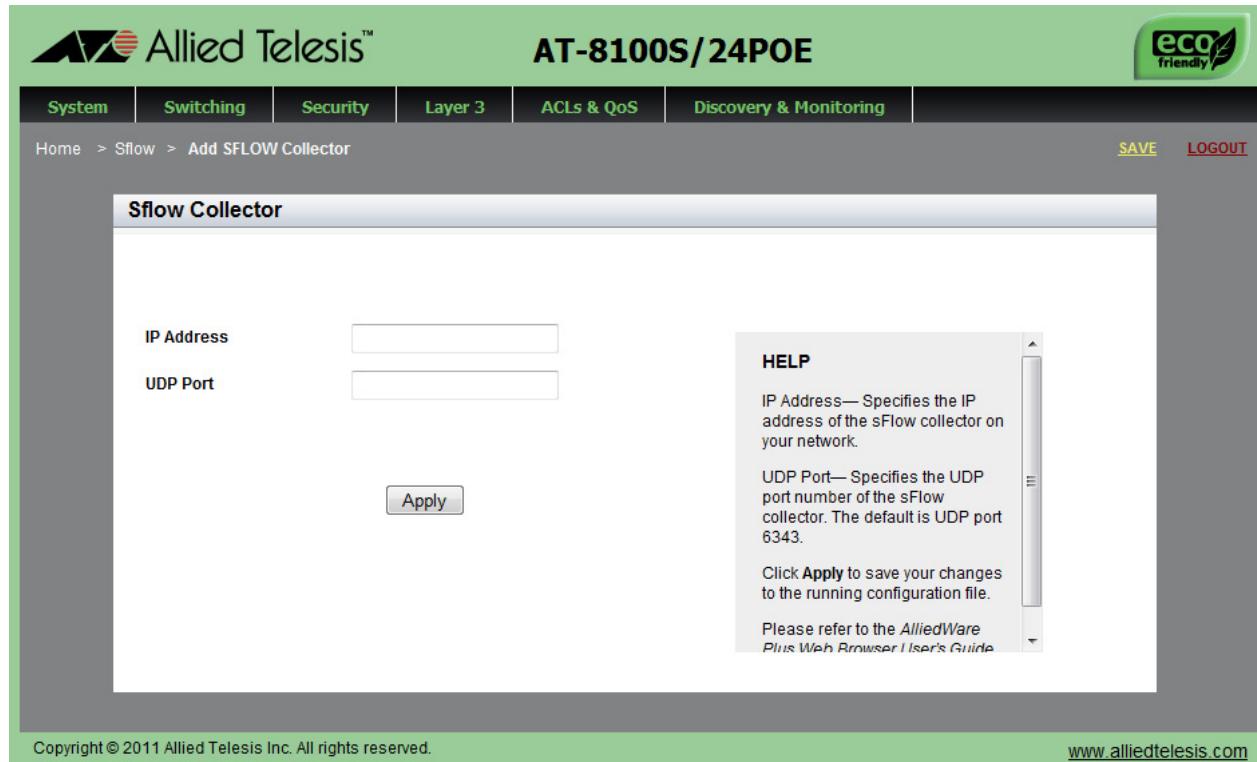


Figure 148. sFlow Collector Page

5. Enter the following fields:

- IP Address**—Enter the IPv4 address of the sFlow collector on your network. Enter the IPv4 address in the following format:

xxx.xxx.xxx.xxx

where x is a number from 0 to 255. There are four groups of numbers that are separated by periods.

- UDP Port**—Enter the UDP port number of the sFlow collector. The default is UDP port 6343.

6. Click **Apply**.7. Click **SAVE** to save your changes to the startup configuration file.

Enabling sFlow on the Switch

Before enabling the sFlow feature on the switch, you must configure sFlow on the ports. The port configurations cannot be edited if the sFlow feature is enabled. For how to configure sFlow on the ports, see “Configuring sFlow on a Port” on page 344.

To enable the sFlow feature on a switch, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 144 on page 344.

2. From the **Discovery & Monitoring** tab, select **sFlow**.

The sFlow page is displayed with the Port Configurations tab selected. See Figure 145 on page 344.

3. Use the pull-down menu next to the **Status** field to select “Enabled.”
4. Click **Apply**.
5. Click **SAVE** to save your changes to the startup configuration file.

Displaying the sFlow Settings

To display the sFlow settings, do the following:

1. Select the **Discovery & Monitoring** tab.

The **Discovery & Monitoring** tab is displayed. See Figure 144 on page 344.

2. From the **Discovery & Monitoring** tab, select **sFlow**.

The sFlow page is displayed with the Port Configurations tab selected. See Figure 145 on page 344.

End of Document